

NETWORK SECURITY FOR WIRELESS AND NON-WIRELESS SYSTEMS

151204

**A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of
Dokuz Eylül University
In Partial Fulfillment of the Requirements for
the Degree of Master of Science in Electric-Electronic Engineering**

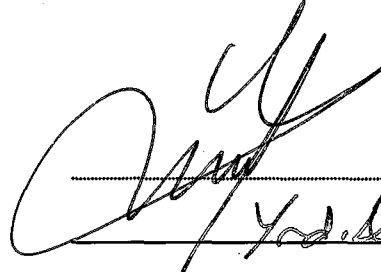
by
Uğur GÜL


151204

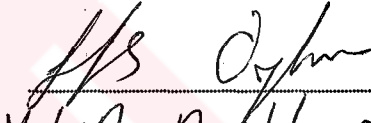
**July, 2004
İZMİR**

M.Sc THESIS EXAMINATION RESULT FORM

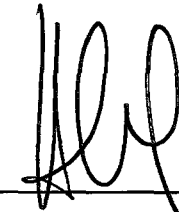
We certify that we have read this thesis and “**NETWORK SECURITY FOR WIRELESS AND NON-WIRELESS SYSTEMS**” completed by **Uğur GÜL** under supervision of **Asos. Prof. Dr. Zafer DİCLE** and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.


Yrd. Doç. Dr. Zafer DİCLE
Supervisor


Doç. Dr. Yalçın ÇEBİ
(Committee Member)



Yrd. Doç. Dr. Hacer Öztuna
(Committee Member)

Approved by the
Graduate School of Natural and Applied Sciences


Prof. Dr. Cahit HELVACI
Director

ACKNOWLEDGMENTS

I would like to thank my supervisor Yrd.Doç.Dr. Zafer DİCLE for his valuable guidance and support during the course of this thesis. I wish to express my sincere appreciation to Rsrch Asst Adnan KAYA and Edip BİNER for their helpful advice. Finally, I thank to my parents and my friends Hakan KARACA and Erman UZUN for their understanding and never ending support throughout my life.



Uğur GÜL

ABSTRACT

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become "wired", an increasing number of people need to understand the basics of security in a networked world. The first part of this document is explaining the local area network, the security principles and understand risks and how to deal with them.

Also it is considered that risk management, network threats, firewalls, and more special-purpose secure networking devices.

As for the wireless , wireless technologies have become increasingly popular in our everyday business and personal lives. Cell phones offer users a freedom of movement unimaginable just over 10 years ago. Personal Digital Assistants (PDA) allow individuals to access calendars, e-mail, address and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years.

An increasing number of government agencies, businesses, and home users are using, or considering using, wireless technologies in their environments. However, these groups need to be aware of the security risks associated with wireless technologies. They need to develop strategies that help mitigate those risks as they integrate these technologies in their computing environments.

The second part of this document discusses wireless technologies, outlines the associated risks, and offers guidance for mitigating those risks.

Keywords : Network, Firewall, IPSec, Wireless, Security, Wep, Bluetooth



ÖZET

Network güvenliği komplike bir yapıya sahiptir ve tecrübe gerektirir. Pek çok insan kablolu ağ kullanmaya başladı başlayalı network dünyasındaki güvenliğin önemini anlayan kişilerin sayısıda artmaya başladı. Bu tezin ilk kısmında yerel ağlar, güvenlik prensipleri, tehditler ve bunlarla nasıl başa çıkacağımız anlatılıyor. Ayrıca risk yönetimi, network tehditleri, ateş duvarı ve bunların özelliklerinede değinildi.

Kablosuz ağlara gelince, kablosuz teknoloji iş ve kişisel yaşamda yavaş yavaş yerini almaya başladı. Cep telefonları kullanıcılara 10 yıl öncesine kadar serbest bir dolaşım imkanı sunuyordu. Aynı şekilde cep bilgisayarlarıda kablosuz olarak internete erişim ve mail alıp vermeyi mümkün kılıyordu. GPS gibi bazı teknolojiler ise dünya üzerinde istediğimiz noktanın yerini bulmamızı sağlayan çok önemli bir teknolojidir. Gelecek yıllarda kablosuz teknoloji bize daha fazla imkanlar sunmaya devam edecek.

Gittikçe bu alandaki kullanıcı sayısının artması ile birlikte kablosuz cihazlar insanların çevrelerinde sıkça kullanılmaya başlandı. Bununla beraber insanlar kablosuz teknolojilerdeki güvenlik açıklarına dikkat etmeye başladılar ve bu konuda insanlar belli güvenlik stratejileri oluşturma ve kablosuz güvenliği sağlama ihtiyacı hissettiler.

Bu tezin ikinci kısmında kablosuz teknolojileri, riskleri ve bunları çözmek için neler yapmamız gerektiğini anlatıyor.

Anahtar sözcükler : Ağ, Ateş Duvarı, IPSec, Kablosuz, Güvenlik, Wep, Bluetooth

CONTENTS

	Page
Contents.....	V
List of Tables.....	XI
List of Figures.....	XII
Introduction.....	1

Chapter One COMPUTER SECURITY

1.Computer security	3
1.1 Lock the doors to the inter-connected world.....	4
1.2 Know who your users are.....	4
1.3 Why should we care about computer security?	4
1.4 Who would want to break into my computer at home?.....	5
1.4.1 How easy is it to break into my computer?.....	5

Chapter Two NETWORK TECHNOLOGY

2. Technology.....	7
2.1 What is a protocol?.....	7
2.2 What is a IP?.....	7
2.3 What is an IP address?.....	7
2.4 What are static and dynamic addressing?.....	8
2.5 What is NAT?.....	9
2.6 What are TCP and UDP ports ?.....	9

Chapter Three

SECURITY RISKS

3. Computer security risks to home users.....	10
3.1 What is risk.....	10
3.2 Actions home users can take to protect their computer systems.....	11

Chapter Four

IP SECURITY

4. IPSEC.....	15
4.1 Introduction.....	15
4.2 What IPsec Does.....	15
4.3 How IPsec Works.....	17
4.3.1 Diagramming a Basic Deployment.....	17
4.4 Examining the Role of IPsec in a Network.....	18
4.5 Enabling IPsec.....	19
4.5.1 Creating a Custom Console.....	20
4.5.2 Enabling Audit Policy for Your Computer.....	21
4.5.3 Configuring the IP Security Monitor.....	22
4.6 Using a Built-in IPsec Policy.....	22
4.7 Impact of Secure Server Policy on a Computer.....	24
4.8 Allowing Non-IPsec clients to talk with a server.....	25
4.9 Configuring IPsec for Security Between Computers.....	25
4.10 Configuring IPsec for Security Between Networks.....	26
4.11 Choosing an IPsec Encryption Scheme.....	27
4.12 Testing an IPsec Policy Assignment.....	28

Chapter Five

FIREWALL

5. Firewall.....	30
5.1 Background and Firewall Basics.....	30
5.1.1 What is a network firewall?.....	30
5.1.2 Why would we need a firewall?.....	31
5.1.3 What can a firewall protect against ?.....	31
5.1.4 What can't a firewall protect against?.....	32
5.1.5 What about viruses?.....	34
5.1.6 Will IPSEC make firewalls obsolete?.....	35
5.2 Design and Implementation Issues.....	36
5.2.1 What are some of the basic design decisions in a firewall?.....	37
5.2.2 Firewall Classes.....	37
5.2.3 Hardware Requirements.....	50
5.2.4 What are proxy servers and how do they work?.....	51
5.2.5 What are the critical resources in a firewall?.....	52
5.2.6 What is a DMZ, and why do we want one?.....	53
5.2.7 How might we increase the security and scalability of my DMZ.....	54
5.2.8 What is a 'single point of failure', and how to avoid having one.....	56
5.2.9 How to block all of the bad stuff?.....	56
5.3 Various Attacks.....	57
5.3.1 What is source routed traffic and why is it a threat?.....	57
5.3.2 What are ICMP redirects and redirect bombs?.....	57
5.3.3 What about denial of service?.....	58
5.3.4 What are some common attacks, and how to protect?.....	59
5.4 How Do We.....	61
5.4.1 Do we really want to allow everything that our users ask for? ...	61
5.4.2 How do we make Web/HTTP work through my firewall?.....	61
5.4.3 How do we make SSL work through the firewall?.....	62
5.4.4 How do we make DNS work with a firewall?.....	62
5.4.5 How do we make FTP work through my firewall?.....	64

5.4.6 How do we make Telnet work through my firewall?.....	65
5.4.7 How do we make Finger and whois work through my firewall?..	65
5.4.8 How do we make gopher, archie work through my firewall?.....	66
5.4.9 How do we make RealAudio work through our firewall?.....	66
5.4.10 How Do we Make IP Multicast Work With our Firewall?.....	67
5.5 Useful Knowledge.....	67
5.5.1 What is a port?.....	67
5.5.2 How do we know which application uses what port?.....	68
5.5.3 What are LISTENING ports?.....	68
5.5.4 How do we determine what service the port is for?.....	69
5.5.5 What ports are safe to pass through a firewall?.....	70
5.5.6 The behavior of FTP.....	71
5.5.7 What software uses what FTP mode?.....	72
5.5.8 Is our firewall trying to connect outside?.....	73

Chapter Six

WIRELESS TECHNOLOGY

6. Overview of Wireless Technology.....	74
6.1 Wireless Networks.....	75
6.1.1 Wireless LANs.....	75
6.1.2 Ad Hoc Networks.....	76
6.2 Wireless Devices.....	77
6.2.1 Personal Digital Assistants.....	77
6.2.2 Smart Phones.....	78
6.2.3 Text-Messaging Devices.....	78
6.3 Wireless Standards.....	78
6.3.1 IEEE 802.11.....	79
6.3.2 Bluetooth.....	80
6.4 Wireless Security Threats and Risk Mitigation.....	81
6.5 Emerging Wireless Technologies.....	84

Chapter Seven

WIRELESS LANs

7. Wireless LANs.....	85
7.1 Wireless LAN Overview.....	85
7.1.1 Brief History.....	86
7.1.2 Frequency and Data Rates.....	87
7.1.3 Architecture.....	87
7.1.4 Wireless LAN Components.....	90
7.1.5 Range.....	91
7.2 Benefits.....	93
7.3 Security of 802.11 Wireless LANS.....	94
7.3.1 Security of the WEP algorithm.....	95
7.3.2 Security Features of 802.11 Wireless LANS per the Standards...	98
7.3.3 Problems with the IEEE 802.11b Standard Security.....	104
7.4 Security Requirements and Threats.....	107
7.4.1 Loss of Confidentiality.....	109
7.4.2 Loss of Integrity	112
7.4.3 Loss of Network Availability.....	112
7.4.4 Other Security Risks.....	113
7.5 Risk Mitigation.....	114
7.5.1 Management Countermeasures.....	114
7.5.2 Operational Countermeasures.....	115
7.5.3 Technical Countermeasures.....	117
7.6 Emerging Security Standards and Technologies.....	135
7.7 Design: Implementing a Wireless LAN in the Work Environment.....	137
7.8 Wireless LAN Security Checklist.....	141

Chapter Eight

ADHOC NETWORKS

8. Ad Hoc Networks.....	144
8.1 Bluetooth Overview.....	145
8.1.1 Bluetooth Architecture and Components.....	148
8.1.2 Frequency and Data Rates.....	149
8.1.3 Range.....	150
8.2 Benefits.....	151
8.3 Bluetooth Security Architecture.....	153
8.3.1 Security Modes.....	153
8.3.2 Security Levels.....	154
8.4 The Bluetooth Protocol Stack.....	155
8.4.1 Security Functions at Bluetooth Protocol Layers.....	156
8.5 Security Manager.....	158
8.6 Authentication.....	159
8.7 Encryption.....	160
8.8 Risks and Limitations.....	161

Chapter Nine

HANDLED DEVICE

9. Handheld Device Security.....	163
9.1 Integrity Concerns.....	164
9.2 Availability Concerns.....	165
9.3 Confidentiality Concerns.....	165
CONCLUSIONS.....	167
REFERENCES.....	172

LIST OF TABLES

	Page
Table 5.1 Class 1-Personal Firewalls.....	40
Table 5.2 Class 2-Router Firewalls.....	42
Table 5.3 Class 3-Low-End Hardware Firewall.....	44
Table 5.4 Class 4-High-End Hardware Firewall.....	46
Table 5.5 Class 5-High-End Server Firewall.....	49
Table 5.6 Hardware Firewall versus Software.....	51
Table 5.7 Critical Resources for Firewall Services.....	53
Table 7.1 Key Characteristics of 802.11 Wireless LANs	86
Table 8.1 Key Characteristics of Bluetooth Technology 5.....	146
Table 8.2 Device Classes of Power Management.....	150

LIST OF FIGURES

	Page
Figure 4.1 Example of a Windows IP Security Development.....	17
Figure 4.2 Examining the role of IPSec in Network 10.....	19
Figure 4.3 Enabling IPSec on Windows 2000.....	19
Figure 4.4 Navigating to Audit Policy in the IPSec console	21
Figure 4.5 Ping indicates IP security negotiation.....	23
Figure 4.6 Successful ping replies.....	24
Figure 4.7 Configuring IPSec for Security Between Computers.....	26
Figure 4.8 Configuring IPSec for Security Between Networks	27
Figure 6.1 Ad Hoc Network.....	77
Figure 7.1 Fundamental 802.11b Wireless LAN Topology.....	89
Figure 7.2 802.11b Wireless LAN Ad Hoc Topology.....	90
Figure 7.3 Typical range of 802.11 WLAN.....	91
Figure 7.4 Access Point Bridging.....	93
Figure 7.5 Wireless Security of 802.11b in Typical Network.....	95
Figure 7.6 Basic WLAN Architecture with 128 bit key.....	96
Figure 7.7 Encrypted Wep frame.....	97
Figure 7.8 Taxonomy of 802.11b Authentication Techniques.....	99
Figure 7.9 Shared key Authentication Message Flow.....	101
Figure 7.10 Wep Privacy using RC4 Algorithm.....	102
Figure 7.11 Key Problem with Existing 802.11 WLAN Security.....	106
Figure 7.12 Taxonomoy of Security Attacks.....	108

Figure 7.13 Typical use of VPN for secure Communications from site to site....	127
Figure 7.14 VPN Security in addition to Wep.....	129
Figure 7.15 Simplified Diagram of VPN WLAN.....	130
Figure 7.16 Unsecured Wireless Access.....	134
Figure 7.17 Typical Smartgate Secured Architecture.....	134
Figure 7.18 Organization A WLAN Architecture.....	140
Figure 7.19 Wireless LAN Security Checklist.....	142
Figure 8.1 Typical Bluetooth Network.....	147
Figure 8.2 Bluetooth Ad Hoc topology.....	149
Figure 8.3 Bluetooth Operating Range.....	151
Figure 8.4 Bluetooth Stack.....	155
Figure 8.5 Bluetooth Security Architecture.....	158
Figure 9.1 RSA.....	164

Introduction

Network Security has become a very important area both for the Research Community and the User Community. The second group is large; anybody who is connected to the Internet through some connection scheme is part of this group. And they face all types of security problems. It is the job of the first group, the Research group, which is constantly at work, to find solution to different problems faced by the user in the area of network security. At present it is a tough situation. More and more people use the Internet and more the net technology and protocols improve; smarter hackers, intruders, spammers try to create more and more problem.

With the advance of technology, another branch of network has emerged, the Mobile and Ad Hoc Network. Security issues become tougher to handle as this new networks have no centralized control.

I propose to deliver this thesis in two parts. First part talks about security issues for standard wired network. It provides background knowledge of networking and protocols, including TCP/IP and UDP and the solution advices. I also talk about how to develop security measures against such attacks. Next I tackle the issues of IpSec and its applications. Next I describe firewalls and its application field. I conclude this part How do we and useful knowledge section where you can find most of the problems about firewall, security and explanations about the most popular security issues.

Wireless technology offers a more accessible means of connectivity, portability and flexibility, increased productivity, lower installation costs, ease of use etc. On the other hand the wireless technology introduces new concerns such as how to address the security concerns involved with offering this less restrained service.

With the deployment of wireless network access in the workplace and private residences, the requirement for a more enhanced security design becomes apparent.

For instance, many organizations that are considering deployment of wireless LANs have major concern about its security, beside other issues, such as performance and scalability of the wireless network implementations.

Businesses that want to implement wireless technologies need to develop strategies that help diminish those security risks as they integrate these technologies in their computing environments.

The second part talks about security in Wireless Lan, Ad Hoc and Mobile Network arena. You can learn how we can protect our network using wep encryption Security Requirements and Threats , Risk Mitigation and a simple design a Wireless LAN in the Work Environment.



CHAPTER ONE

COMPUTER SECURITY

1. Computer security

An Internet connection is rapidly becoming an essential for today's companies and organisations. The advantages and commercial benefits are well known and recognised across all business sectors. Companies of all sizes are seeking a pro-active presence on the web and most now rely on email for quick and efficient business communications. The advent of e-commerce will only deepen the impact the Internet is having on our rapidly changing business world. The one thing that remains amidst all the change is the natural concern about security. An Internet connection opens up corporate networks to the world and there are people out there who want to see what you have and potentially they can wreak havoc with systems, private data and critical records.

Fortunately the development of Internet and Network security technology has mirrored the growth of the Internet. A thriving business sector on its own, Network security has become big business with many of the world's leading software developers playing an active part and generating some of the most significant technological innovations of recent times. For example, for every new virus there is an appropriate software update available to download from web sites to counteract the threat.

Customer confidence in the Internet is building, as the growth in e-commerce transactions and the deployment of critical VPNs testifies.

Whilst the threats remain and are real the solutions employed are effective and are helping build consumer confidence. Looking at each of the security concerns in turn allows us to identify the solutions on offer.

1.1 Lock the doors to the inter-connected world.

Connecting your network to the public Internet really opens the doors to the interconnected world. Your network has to be protected from hackers, malicious attack and other unauthorised access.

Firewalls, perimeter security and intrusion detection systems, backed up by automatic responses with detailed logging and alerting procedures are the heart of any enterprise security system. A firewall is essential to network security if unauthorised access is to be denied.

1.2 Know who your users are.

Connections into and out of your network need to be strictly controlled. Allowing access through the firewall to known personnel is required if business communication is to effectively use the Internet. The management of these connections forms a major part of the enterprise security policy. The key security issue is authentication, knowing who your users really are. Software and hardware solutions are deployed to authenticate both machines and users. Repeated checks are made during sessions to ensure that only authorised users can have access to your data and systems.

1.3 Why should we care about computer security?

We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs.

Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer (such as financial statements).

1.4 Who would want to break into my computer at home?

Intruders (also referred to as hackers, attackers, or crackers) may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.

Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems. Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target.

Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.

1.4.1 How easy is it to break into my computer?

Unfortunately, intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

When holes are discovered, computer vendors will usually develop patches to address the problem(s). However, it is up to you, the user, to obtain and install the patches, or correctly configure the software to operate more securely..

Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure.

Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.



CHAPTER TWO

NETWORK TECHNOLOGY

2. Technology

2.1 What is a protocol?

A protocol is a well-defined specification that allows computers to communicate across a network. In a way, protocols define the "grammar" that computers can use to "talk" to each other. (WEB_1. 2004)

2.2 What is IP?

IP stands for "Internet Protocol". It can be thought of as the common language of computers on the Internet. There are a number of detailed descriptions of IP given elsewhere, so we won't cover it in detail in this document. However, it is important to know a few things about IP in order to understand how to secure your computer. Here we'll cover IP addresses, static vs. dynamic addressing, NAT, and TCP and UDP Ports

2.3 What is an IP address?

IP addresses are analogous to telephone numbers – when you want to call someone on the telephone, you must first know their telephone number.

Similarly, when a computer on the Internet needs to send data to another computer, it must first know its IP address.

IP addresses are typically shown as four numbers separated by decimal points, or “dots”. For example, 10.24.254.3 and 192.168.62.231 are IP addresses.

If you need to make a telephone call but you only know the person’s name, you can look them up in the telephone directory (or call directory services) to get their telephone number. On the Internet, that directory is called the Domain Name System, or DNS for short. If you know the name of a server, say www.cert.org, and you type this into your web browser, your computer will then go ask its DNS server what the numeric IP address is that is associated with that name.

Every computer on the Internet has an IP address associated with it that uniquely identifies it. However, that address may change over time, especially if the computer is dialing into an Internet Service Provider (ISP) connected behind a network firewall connected to a broadband service using dynamic IP addressing.

2.4 What are static and dynamic addressing?

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time. However, if a static address is assigned but not in use, it is effectively wasted. Since ISPs have a limited number of addresses allocated to them, they sometimes need to make more efficient use of their addresses.

Dynamic IP addressing allows the ISP to efficiently utilize their address space. Using dynamic IP addressing, the IP addresses of individual user computers may change over time. If a dynamic address is not in use, it can be automatically reassigned to another computer as needed.

2.5 What is NAT?

Network Address Translation (NAT) provides a way to hide the IP addresses of a private network from the Internet while still allowing computers on that network to access the Internet. NAT can be used in many different ways, but one method frequently used by home users is called "masquerading".

Using NAT masquerading, one or more devices on a LAN can be made to appear as a single IP address to the outside Internet.

This allows for multiple computers in a home network to use a single cable modem or DSL connection without requiring the ISP to provide more than one IP address to the user. Using this method, the ISP-assigned IP address can be either static or dynamic. Most network firewalls support NAT masquerading.

2.6 What are TCP and UDP Ports?

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both protocols that use IP. Whereas IP allows two computers to talk to each other across the Internet, TCP and UDP allow individual applications (also known as "services") on those computers to talk to each other. In the same way that a telephone number or physical mail box might be associated with more than one person, a computer might have multiple applications (e.g. email, file services, web services) running on the same IP address. Ports allow a computer to differentiate services such as email data from web data. A port is simply a number associated with each application that uniquely identifies that service on that computer. Both TCP and UDP use ports to identify services. Some common port numbers are 80 for web (HTTP), 25 for email (SMTP), and 53 for Domain Name System (DNS).

CHAPTER THREE

SECURITY RISKS

3. Computer security risks to home users

3.1 What is at risk?

Information security is concerned with three main areas:

Confidentiality - information should be available only to those who rightfully have access

Integrity -- information should be modified only by those who are authorized to do so

Availability -- information should be accessible to those who need it when they need

These concepts apply to home Internet users just as much as they would to any corporate or government network. You probably wouldn't let a stranger look through your important documents. In the same way, you may want to keep the tasks you perform on your computer confidential, whether it's tracking your investments or sending email messages to family and friends. Also, you should have some assurance that the information you enter into your computer remains intact and is available when you need it (WEB_2. 2004)

Some security risks arise from the possibility of intentional misuse of your computer by intruders via the Internet. Others are risks that you would face even if you weren't

connected to the Internet (e.g. hard disk failures, theft, power outages). The bad news is that you probably cannot plan for every possible risk.

The good news is that you can take some simple steps to reduce the chance that you'll be affected by the most common threats -- and some of those steps help with both the intentional and accidental risks you're likely to face.

3.2 Actions home users can take to protect their computer systems

It is recommends the following practices to home users:

- * Consult your system support personnel if you work from home
 - * Use virus protection software
 - * Use a firewall
 - * Don't open unknown email attachments
 - * Don't run programs of unknown origin
 - * Disable hidden filename extensions
 - * Keep all applications (including your operating system) patched
 - * Turn off your computer or disconnect from the network when not in use
 - * Disable Java, JavaScript, and ActiveX if possible
 - * Disable scripting features in email programs
 - * Make regular backups of critical data
 - * Make a boot disk in case your computer is damaged or compromised
- * Consult your system support personnel if you work from home : If you use your broadband access to connect to your employer's network via a Virtual Private Network (VPN) or other means, your employer may have policies or procedures relating to the security of your home network..
- * Use virus protection software : It is recommended the use of anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date.

Many anti-virus packages support automatic updates of virus definitions. We recommend the use of these automatic updates when available

* Use a firewall : We strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks. However, no firewall can detect or stop all attacks, so it's not sufficient to install a firewall and then ignore all other security measures.

* Don't open unknown email attachments : Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs.

If you must open an attachment before you can verify the source, we suggest the following procedure:

be sure your virus definitions are up-to-date

save the file to your hard disk

scan the file using your antivirus software

open the file

For additional protection, you can disconnect your computer's network connection before opening the file. Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.

* Don't run programs of unknown origin : Never run a program unless you know it to be authored by a person or company that you trust.

Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

* **Disable hidden filename extensions :** Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but you can disable this option in order to have file extensions displayed by Windows. After disabling this option, there are still some file extensions that, by default, will continue to remain hidden.

There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system. The "NeverShowExt" registry value is used to hide the extensions for basic Windows file types. For example, the ".LNK" extension associated with Windows shortcuts remains hidden even after a user has turned off the option to hide extensions.

* **Keep all applications, including your operating system, patched :** Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches.

You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information. Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check periodically for updates.

* **Turn off your computer or disconnect from the network when not in use :** Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

* **Disable Java, JavaScript, and ActiveX if possible :** Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Turning off these options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some web sites.

Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites.

* **Disable scripting features in email programs :** Because many email programs use the same code as web browsers to display HTML, vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to email as well as web pages. It is recommended that users also disable these features in their email programs.

* **Make regular backups of critical data :** Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store the backup disks somewhere away from the computer.

* **Make a boot disk in case your computer is damaged or compromised :** To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk which will help when recovering a computer after such an event has occurred. Remember, however, you must create this disk before you have a security event.

CHAPTER FOUR

IP SECURITY

4.IPSEC

4.1 INTRODUCTION

Without security, both public and private networks are susceptible to unauthorized monitoring and access. Internal attacks might be a result of minimal or nonexistent intranet security, whereas risks from outside the private network system from connections to the internet and extranets. IPsec protects private data in a public environment by providing a strong, cryptography-based defense against network attacks.

IPsec is an internet Engineering Task Force (IETF) proposal and is not yet an IETF standard. IPsec is developed by a working group of the same name within the IETF (Internet Engineering Task Force). This group was created in 1992 and a first version of the proposed mechanisms was published in the form of RFCs in 1995. This first version didn't include the key management part, which is more recent. Key management was included in the new IPsec RFCs that came out in November 1998. But IPsec remains an evolving standard, which is still subject to multiple Internet drafts..

4.2 What IPsec Does

IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. (The term "security gateway" is used throughout the IPsec documents to refer to an intermediate system that implements IPsec protocols. For example, a router or a firewall implementing IPsec is a security gateway.)

The set of security services that IPsec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, etc.

The IPsec DOI also supports negotiation of IP compression [SMPT98], motivated in part by the observation that when encryption is employed within IPsec, it prevents effective compression by lower protocol layers.

IP Security, as defined by the Internet Engineering Task Force (IETF), uses an authentication header (AH) and an encapsulated security payload (ESP). The authentication header provides data communication with source authentication and integrity. The encapsulated security payload provides confidentiality, in addition to authentication and integrity. With IP Security, only the sender and recipient know the security key. If the authentication data is valid, the recipient knows that the communication came from the sender and that it was not changed in transit.

Windows IP Security builds upon the IETF model by mixing public-key and secret-key cryptography and by providing automatic key management for maximized security and high-speed throughput.

This gives a combination of authentication, integrity, anti-replay, and (optionally) confidentiality to ensure secure communications.

The security policies assigned to Host A and Host B by the administrator determine the level of security for the communication. These are picked up by the policy agent and passed to the ISAKMP/Oakley service and IPSEC driver. The ISAKMP/Oakley service on each computer uses the negotiation policies associated with the assigned security policy to establish the key and a common negotiation method (a security association). The results of the ISAKMP policy negotiation between the two computers are passed to the IPSEC driver, which uses the key to encrypt the data. Finally, the IPSEC driver sends the encrypted data to Host B. The IPSEC driver on Host B decrypts the data and passes it up to the receiving application.

4.4 Examining the Role of IPSec in a Network

The primary goal of IPSec is to provide protection for IP packets. IPSec is based on an end to end security model, meaning that the sender and the receiver are the only hosts that must know about the IPSec protection. Each computer handles security at its own end under the assumption that the medium over which the communication takes place is not secure. Computers that only route data from source to destination are not required to support IPSec.

IPSec is implemented by using an IPSec policy. Policies are security settings, or rules, that define the level of security that you want, in addition to the address, protocols, Domain Name Systems (DNS) names, subnets, or connection types to which the security settings will apply. The IPSec driver matches every incoming and outgoing packet against the security settings defined in the active IPSec policy.

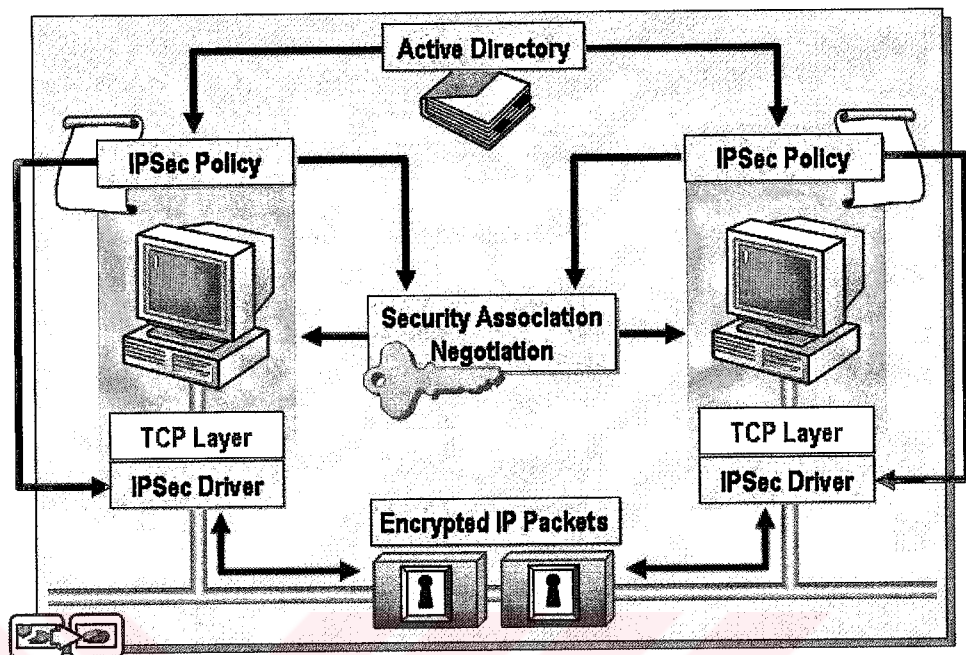


Figure 4.2 Examining the role of IPsec in Network

4.5 Enabling IPsec

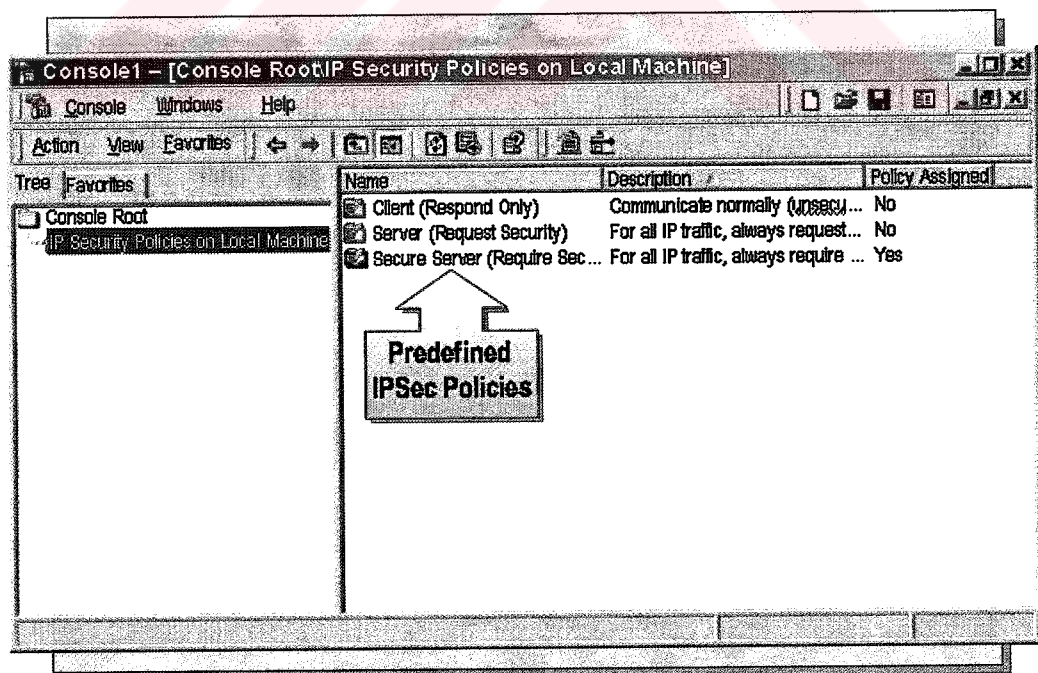


Figure 4.3 Enabling IPsec on Windows 2000

You can control IPsec by using a policy configuration that you manage in IP Security Policy Management. You use IP Security Policy Management to manage IPsec to manage IPsec policies centrally for Active Directory clients, locally for the computer on which you are running the console, or remotely for a computer or domain.

To activate an IPsec policy on a management ; In Ip Security Policy Management click IP Security Policies on Local Machine and then in the details pane, right click the policy that you want to assign, and then click assign.

4.5.1 Creating a Custom Console

Log on to the first test computer as a user with administrative privileges. In our example, this is the computer named HQ-RES-WRK-01.

Note: For the remainder of this document, HQ-RES-WRK-01 will refer to the first test computer, and HQ-RES-WRK-02 will refer to the second test computer. If your machines have different names, be sure and track the steps using the proper name.

4.5.1.1 Create a custom MMC console

1-From the Windows desktop, click **Start**, click **Run**, and in the **Open** textbox type **mmc**. Click **OK**

2-On the **Console** menu, click **Add/Remove Snap-in**.

3-In the **Add/Remove Snap-in** dialog box, click **Add**.

4-In the **Add Standalone Snap-in** dialog box, click **Computer Management**, and then click **Add**.

5-Verify that **Local Computer** is selected, and click **Finish**.

6-In the **Add Standalone Snap-in** dialog box, click **Group Policy**, and then click **Add**.

7-Verify that **Local Computer** is selected in the **Group Policy Object** dialog box, and click **Finish**.

8-In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.

9-Select **Computer Account**, and click **Next**.

10-Verify that **Local Computer** is selected, and click **Finish**.

11-To close the **Add Standalone Snap-in** dialog box, click **Close**.

12-To close the **Add/Remove Snap-in** dialog box, click **OK**.

4.5.2 Enabling Audit Policy for Your Computer

In the next procedure, you will configure auditing, so that an event will be logged when IPSec is involved in communication. Later, this will be a useful confirmation that IPSec is working properly.

To enable audit policy

1- In the **MMC console**, select **Local Computer Policy** from the left pane and click + to expand the tree. Navigate to **Computer Configuration**, to **Windows Settings**, to **Security Settings**, then to **Local Policies**, and select **Audit Policy**.

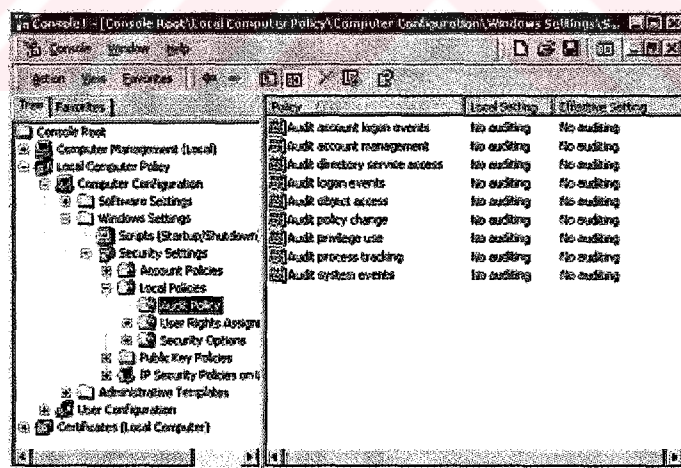


Figure 4.4 Navigating to Audit Policy in the IPSec Console

2-From the list of **Attributes** displayed in the right pane, double-click **Audit Logon Events**. The **Audit Logon Events** dialog box appears.

3-In the **Audit Logon Events** dialog box, click to select both the **Audit these attempts: Success** and **Failed** check boxes, and click **OK**.

4-Repeat steps 2 and 3 for the **Audit Object Access** attribute.

4.5.3 Configuring the IP Security Monitor

To monitor the successful security connections that the IPSec policy will create, use the IP Security Monitor tool. Before creating any policies, first start and configure the tool.

To start and configure the IP Security Monitor

1-To start the IP Security Monitor tool, click **Start**, click **Run**, and type **ipsecmon** into the **Open** text box. Click **OK**.

2-Click **Options** in the IP Security Monitor tool, and change the default value for **Refresh Seconds** from 15 to 1. Click **OK**.

3-Minimize the **IP Security Monitor** window.

You will use this minimized tool to monitor the policies later in this walkthrough.

Return to the beginning of this section, Creating a Custom Console and repeat all steps to this point for the second computer (in our example, this is the machine named HQ-RES-WRK-02).

4.6 Using a Built-in IPSec Policy

In this exercise, you will activate one of the built-in IPSec policies to secure traffic between the two computers. The default policies use Kerberos as the initial authentication method. Because both machines are members of a Windows 2000 domain, a minimal amount of configuration is required.

To activate the policy on HQ-RES-WRK-01:

1-In the **MMC** console you created earlier, select **IP Security Policies on Local Machine** from the left pane. There are three entries in the right pane: **Client**, **Secure Server**, and **Server**.

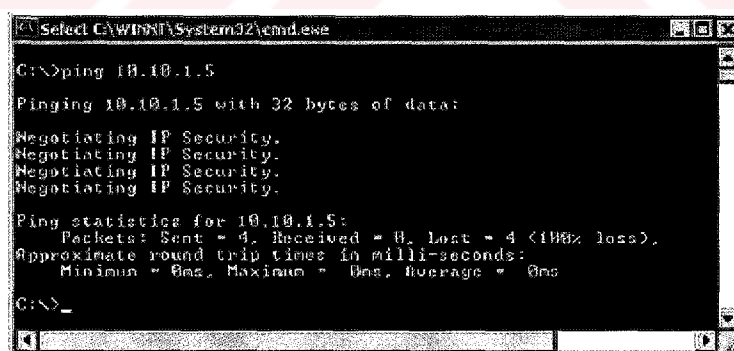
2-Right-click **Secure Server**, and then choose **Assign**. The status in the **Policy Assigned** column should change from **No** to **Yes**.

3-Repeat step 1 on HQ-RES-WRK-02. Right-click **Client**, and then choose **Assign**. The status in the **Policy Assigned** column changes from **No** to **Yes**.

Now you have one computer (HQ-RES-WRK-01) acting as a secure server, and the other (HQ-RES-WRK-02) acting as a client. The client will initially send unprotected ICMP Echo packets (using the ping utility) to the server, but the server will request security from the client, after which the rest of the communication will be secure. If the server were to initiate the ping, then the ping would have to be secured to the client before the server would allow it on the network.

If the client computer had a secure server policy as well, it would not send unprotected pings or any other traffic; rather, it would request IPsec protection before any application data was sent. If both computers had client policies, no data would be protected, because neither side requests security.

4- On HQ-RES-WRK-02, click **Start**, click **Run**, type **cmd** in the text box, and click **OK**. Type **ping IP1** (the IP address of HQ-RES-WRK-01). In this example, IP1 is 10.10.1.5. As shown in figure below, the ping response will indicate that IPsec is being negotiated.



```

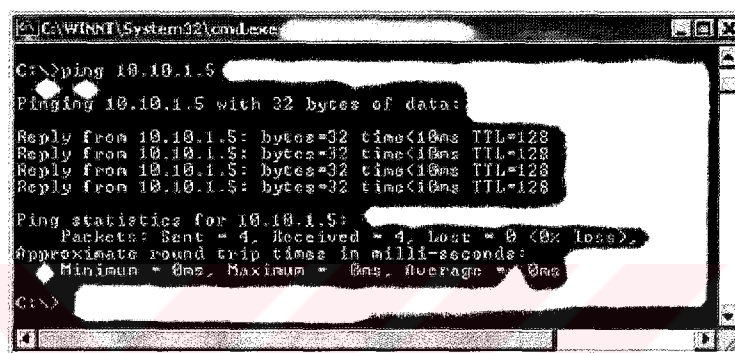
Select C:\WINNT\System32\cmd.exe
C:\>ping 10.10.1.5
Pinging 10.10.1.5 with 32 bytes of data:
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Ping statistics for 10.10.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>_
  
```

Figure 4.5 Ping Indicates IP Security Negotiation

5-Restore the **IP Security Monitor** window, which you minimized earlier.

You should see details of the Security Association that is currently in use between your two machines, as well as statistics on the number of Authenticated and Confidential bytes transmitted.

6- Repeat the ping command. Now that the two computers have established IPSec security associations between them, you should receive four successful replies as shown in figure below. In this example, IP1 is 10.10.1.5.



```
C:\WINNT\System32\cmd.exe
C:\>ping 10.10.1.5
Pinging 10.10.1.5 with 32 bytes of data:
Reply from 10.10.1.5: bytes=32 time<10ms TTL=128
Reply from 10.10.1.5: bytes=32 time<10ms TTL=128
Reply from 10.10.1.5: bytes=32 time<10ms TTL=128
Reply from 10.10.1.5: bytes=32 time<10ms TTL=128

Ping statistics for 10.10.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figure 4.6 : Successful ping replies

7-Still working on HQ-RES-WRK-02, from the left pane in the MMC, click the + next to **Computer Management** to expand it, then expand **System Tools**, expand **Event Viewer**, and click **Security Log**. Double-click the top instance of **Success Audit** in the right pane.

You have successfully configured and used IP Security between the two computers.

4.7 Impact of Secure Server Policy on a Computer

Only IPSec clients that can successfully negotiate can communicate with the secure server computer. Also, the secure server will not be able to talk to any other systems, such as Domain Name System (DNS) servers, unless that traffic can be secured using IPSec. Because many services are running in the background on the server, they will probably fail to communicate and generate event log messages.

This is normal, because the default Secure Server policy is very severe and attempts to secure almost all IP packets before letting them into the network. For actual use in production environments, you must create a custom policy that has the behavior you want according to your security requirements, network topology, and specific server application usage.

4.8 Allowing Non-IPSec Clients To Talk with A Server

To allow non-IPSec clients to communicate as well, you should assign the **Server** policy, instead of **Secure Server**. This always requests security, but allows unsecured communication with clients, by falling back to clear text if the client does not reply to the IKE negotiation request. If at any time the client does reply, then a negotiation is in progress and must succeed completely. If negotiation fails the communication will be blocked for one minute, whereupon another negotiation will be attempted. See the section, Configuring an IPSec Filter Action, for more explanation on the settings that are used to control this behavior.

Unassign the **Secure Server** or **Server** and **Client** policies to return your computers to their previous states, by right-clicking the policy in the right pane (under **IP Security Policies on Local Machine** in the left pane), and then clicking **Unassign**.

4.9 Configuring IPSec for Security Between Computers

The Transport mode authenticates and encrypts data flowing between any two computers running Windows 2000. The transport mode provides security for the network and can potentially support a secure connection with more than once computer. Transport mode is the default IPSec mode

■ Using IPSec in Transport Mode

- Enforces IPSec policies for traffic between systems
- Supports Windows 2000
- Provides end-to-end security
- Is the default mode for IPSec

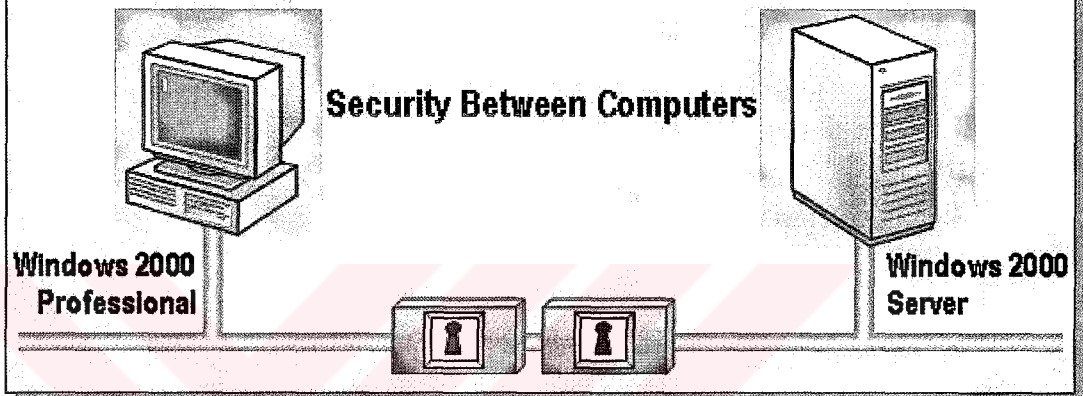


Figure 4.7 Configuring IPSec for Security Between Computers

4.10 Configuring IPSec for Security Between Networks

To create secured communications between remote networks, configure IPSec for tunnel mode. The advantage of tunnel mode is that data is secure between the two tunnel ends, regardless of the ultimate destination.

When you configure IPSec for tunnel mode, all communications between networks are secure, without requiring you to configure IPSec on each computer. Tunnel mode does not provide security within each network.

To specify an IPSec tunnel, open IP Security Policy Management, in the details pane right click the policy that you want to modify then click properties.

Click the rule that you want to modify and then click edit, on the Tunnel setting tab click The Tunnel endpoint is specified by this IP address and then specify the IP address of the tunnel endpoint.

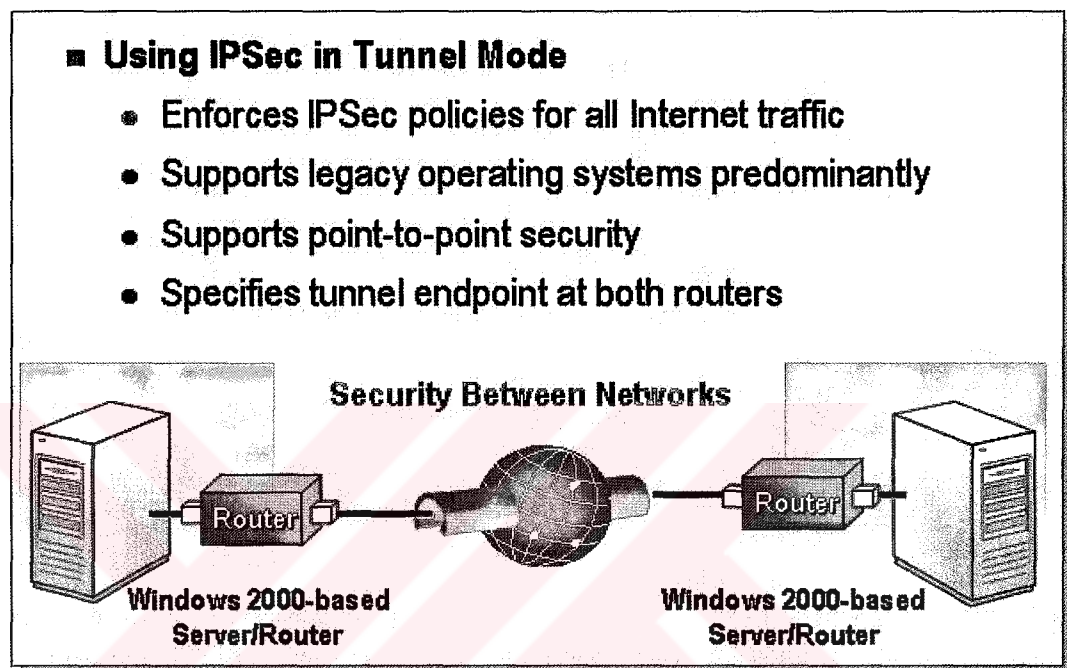


Figure 4.8. Configuring IPSec for Security Between Networks

4.11 Choosing an IPSec Encryption Scheme

4.11.1 Diffie-Hellman (DH) Technique

The Diffie-Hellman Technique (named for its inventors Whitfield Diffie and Martin Hellman) is a public key cryptography algorithm that allows two communicating entities to agree on a shared key. Diffie-Hellman starts with the two entities exchanging public information. Each entity then combines the other's public information along with its own secret information to generate a shared-secret value.

4.11.2 Hash Message Authentication Code (HMAC)

HMAC is a secret-key algorithm providing integrity and authentication. Authentication using keyed hash produces a digital signature for the packet that can be verified by the receiver. If the message changes in transit, the hash value is different and the IP packet is rejected.

4.11.3 HMAC-MD5

Message Digest function 95 (MD5) is a hash function that produces a 128-bit value.

4.11.4 HMAC-SHA

Secure Hash Algorithm (SHA) is a hash function that produces a 160-bit value. While somewhat slower than HMAC-MD5, HMAC-SHA is more secure.

4.11.5 DES-CBC

Data Encryption Standard (DES)—Cipher block chaining (CBC) is a secret key algorithm used for confidentiality. A random number is generated and used with the secret key to encrypt the data.

4.12 Testing an IPSec Policy Assignment

There are two methods to test IPSec ,

Using the Ping command to verify that a valid network connection ; Open a command prompt, type ping Ip address is the IP address of the computer with which you are trying to communicate, and then press enter. If there is a valid network connection, you should receive four replies to the ping.

This verifies that you can communicate with the destination IP address. IPSec does not block the ping command if you are using the default policies unmodified.

Using IPSec Monitor to verify that a policy has been assigned ; IPSec monitor displays the active security associations on local or remote computers. For example, you can use IPSec Monitor to determine whether there is a pattern of authentication or security associations failures, possibly indicating incompatible security policy settings. When IPSec monitor opens, you see a message in the lower right corner indicating whether IPSec is enabled on the computer. For IPSec to be enabled, you must assign a policy.



CHAPTER FIVE

FIREWALL

5. FIREWALL

5.1 Background and Firewall Basics

Before being able to understand a complete discussion of firewalls, it's important to understand the basic principles that make firewalls work.

5.1.1 What is a network firewall?

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. If you don't have a good idea of what kind of access you want to allow or to deny, a firewall really won't help you. It's also important to recognize that the firewall's configuration, because it is a mechanism for enforcing policy, imposes its policy on everything behind it. Administrators for firewalls managing the connectivity for a large number of hosts therefore have a heavy responsibility.

5.1.2 Why would we need a firewall?

The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's walls with spraypaint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. Usually, a firewall's purpose is to keep the jerks out of your network while still letting you get your job done.

Many traditional-style corporations and data centers have computing security policies and practices that must be adhered to. In a case where a company's policies dictate how data must be protected, a firewall is very important, since it is the embodiment of the corporate policy. Frequently, the hardest part of hooking to the Internet, if you're a large company, is not justifying the expense or effort, but convincing management that it's safe to do so. A firewall provides not only real security--it often plays an important role as a security blanket for management.

Lastly, a firewall can act as your corporate ``ambassador" to the Internet. Many corporations use their firewall systems as a place to store public information about corporate products and services, files to download, bug-fixes, and so forth. Several of these systems have become important parts of the Internet service structure (e.g.: UUnet.uu.net, whitehouse.gov, gatekeeper.dec.com) and have reflected well on their organizational sponsors.

5.1.3 What can a firewall protect against?

Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections, and block services that are known to be problems.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the ``outside" world. This, more than anything, helps prevent vandals from logging into machines on your network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. The firewall can protect you against any type of network-borne attack if you unplug it.

Firewalls are also important since they can provide a single ``choke point" where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialing in with a modem, the firewall can act as an effective ``phone tap" and tracing tool. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc.

This is an important point: providing this ``choke point" can serve the same purpose on your network as a guarded gate can for your site's physical premises. That means anytime you have a change in ``zones" or levels of sensitivity, such a checkpoint is appropriate. A company rarely has only an outside gate and no receptionist or security staff to check badges on the way in. If there are layers of security on your site, it's reasonable to expect layers of security on your network.

5.1.4 What can't a firewall protect against?

Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape can just as effectively be used to export data. Many organizations that are terrified (at a management level) of Internet connections have no coherent policy about how dial-in access via modems should be protected.

It's silly to build a 6-foot thick steel door when you live in a wooden house, but there are a lot of organizations out there buying expensive firewalls and neglecting the numerous other back-doors into their network. For a firewall to work, it must be a part of a consistent overall organizational security architecture. Firewall policies must *be* realistic and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the Internet in the first place, or the systems with the really secret data should be isolated from the rest of the corporate network.

Another thing a firewall can't really protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he's just as likely to export it through a telephone, FAX machine, or floppy disk.

Floppy disks are a far more likely means for information to leak from your organization than a firewall! Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering; an attacker may be able to break into your network by completely bypassing your firewall, if he can find a "helpful" employee inside who can be fooled into giving access to a modem pool. Before deciding this isn't a problem in your organization, ask yourself how much trouble a contractor has getting logged into the network or how much difficulty a user who forgot his password has getting it reset. If the people on the help desk believe that every call is internal, you have a problem.

Lastly, firewalls can't protect against tunneling over most application protocols to trojaned or poorly written clients. There are no magic bullets and a firewall is not an excuse to not implement software controls on internal networks or ignore host security on servers. Tunneling "bad" things over HTTP, SMTP, and other protocols is quite simple and trivially demonstrated. Security isn't "fire and forget".

5.1.5 What about viruses?

Firewalls can't protect very well against things like viruses. There are too many ways of encoding binary files for transfer over networks, and too many different architectures and viruses to try to search for them all. In other words, a firewall cannot replace security-consciousness on the part of your users. In general, a firewall cannot protect against a data-driven attack--attacks in which something is mailed or copied to an internal host where it is then executed. This form of attack has occurred in the past against various versions of *sendmail*, *ghostscript*, and scripting mail user agents like OutLook.

Organizations that are deeply concerned about viruses should implement organization-wide virus control measures. Rather than trying to screen viruses out at the firewall, make sure that every vulnerable desktop has virus scanning software that is run when the machine is rebooted. Blanketing your network with virus scanning software will protect against viruses that come in via floppy disks, modems, and Internet. Trying to block viruses at the firewall will only protect against viruses from the Internet--and the vast majority of viruses are caught via floppy disks.

Nevertheless, an increasing number of firewall vendors are offering ``virus detecting'' firewalls. They're probably only useful for naive users exchanging Windows-on-Intel executable programs and malicious-macro-capable application documents. There are many firewall-based approaches for dealing with problems like the ``ILOVEYOU'' worm and related attacks, but these are really oversimplified approaches that try to limit the damage of something that is so stupid it never should have occurred in the first place. Do not count on any protection from attackers with this feature.

A strong firewall is never a substitute for sensible software that recognizes the nature of what it's handling--untrusted data from an unauthenticated party--and behaves .

Do not think that because ``everyone" is using that mailer or because the vendor is a gargantuan multinational company, you're safe. In fact, it isn't true that ``everyone" is using any mailer, and companies that specialize in turning technology invented elsewhere into something that's ``easy to use" without any expertise are more likely to produce software that can be fooled.

5.1.6 Will IPSEC make firewalls obsolete?

Some have argued that this is the case. Before pronouncing such a sweeping prediction, however, it's worthwhile to consider what IPSEC is and what it does. Once we know this, we can consider whether IPSEC will solve the problems that we're trying to solve with firewalls.

IPSEC (IP SECurity) refers to a set of standards developed by the Internet Engineering Task Force (IETF). There are many documents that collectively define what is known as ``IPSEC" IPSEC solves two problems which have plagued the IP protocol suite for years: host-to-host authentication (which will let hosts know that they're talking to the hosts they think they are) and encryption (which will prevent attackers from being able to watch the traffic going between machines).

Note that neither of these problems is what firewalls were created to solve. Although firewalls can help to mitigate some of the risks present on an Internet without authentication or encryption, there are really two classes of problems here: integrity and privacy of the information flowing between hosts and the limits placed on what kinds of connectivity is allowed between different networks. IPSEC addresses the former class and firewalls the latter.

What this means is that one will not eliminate the need for the other, but it does create some interesting possibilities when we look at combining firewalls with IPSEC-enabled hosts.

Namely, such things as vendor-independent virtual private networks (VPNs), better packet filtering (by filtering on whether packets have the IPSEC authentication header), and application-layer firewalls will be able to have better means of host verification by actually using the IPSEC authentication header instead of ``just trusting" the IP address presented.

5.2 Design and Implementation Issues

5.2.1 What are some of the basic design decisions in a firewall?

There are a number of basic design issues that should be addressed by the lucky person who has been tasked with the responsibility of designing, specifying, and implementing or overseeing the installation of a firewall.

The first and most important decision reflects the policy of how your company or organization wants to operate the system: is the firewall in place explicitly to deny all services except those critical to the mission of connecting to the Net, or is the firewall in place to provide a metered and audited method of ``queuing" access in a non-threatening manner? There are degrees of paranoia between these positions; the final stance of your firewall might be more the result of a political than an engineering decision.

The second is: what level of monitoring, redundancy, and control do you want? Having established the acceptable risk level (e.g., how paranoid you are) by resolving the first issue, you can form a checklist of what should be monitored, permitted, and denied. In other words, you start by figuring out your overall objectives, and then combine a needs analysis with a risk assessment, and sort the almost always conflicting requirements out into a laundry list that specifies what you plan to implement.

The third issue is financial. For example, a complete firewall product may cost between \$100,000 at the high end, and free at the low end.

The free option, of doing some fancy configuring on a Cisco or similar router will cost nothing but staff time and a few cups of coffee.

Implementing a high end firewall from scratch might cost several man-months, which may equate to \$30,000 worth of staff salary and benefits. The systems management overhead is also a consideration. Building a home-brew is fine, but it's important to build it so that it doesn't require constant (and expensive) attention. It's important, in other words, to evaluate firewalls not only in terms of what they cost now, but continuing costs such as support.

On the technical side, there are a couple of decisions to make, based on the fact that for all practical purposes what we are talking about is a static traffic routing service placed between the network service provider's router and your internal network. The traffic routing service may be implemented at an IP level via something like screening rules in a router, or at an application level via proxy gateways and services.

The decision to make is whether to place an exposed stripped-down machine on the outside network to run proxy services for telnet, FTP, news, etc., or whether to set up a screening router as a filter, permitting communication with one or more internal machines. There are pluses and minuses to both approaches, with the proxy machine providing a greater level of audit and potentially security in return for increased cost in configuration and a decrease in the level of service that may be provided (since a proxy needs to be developed for each desired service). The old trade-off between ease-of-use and security comes back to haunt us with a vengeance.

5.2.2 Firewall Classes

The following section presents a number of classes of firewalls, each of which provides certain firewall features. Specific firewall classes can be used to respond to specific requirements in the design of an IT architecture.

Grouping firewalls into classes allows for the abstraction of the hardware from the requirements of the service.

Service requirements can then be matched against class features. As long as a firewall fits into a specific class, it can support all of the services that the class of firewalls is required to support. (WEB_3. 2004)

The various classes are as follows:

Class 1 - Personal firewalls

Class 2 - Router firewalls

Class 3 - Low-end hardware firewalls

Class 4 - High-end hardware firewalls

Class 5 - High-end server firewalls

It is important to understand that some of these classes overlap. This is by design, as the overlap allows one type of firewall solution to span multiple classes. Many classes can also be served by more than one hardware model from the same vendor, so that your organization can select a model that suits its present and future requirements. Apart from the price and feature set, firewalls can be classified on the basis of performance (or throughput). However, manufacturers do not provide any figures of throughput for most classes of firewalls. Where they are provided (typically for hardware firewall devices), no standard measurement process is followed, which makes comparisons between manufacturers difficult. For example, one measure is the number of bits per second (bps), but as the firewall is actually passing IP packets, this measure is meaningless if the packet size used in measuring the rate is not included.

The following subsections define firewall classes in detail.

5.2.2.1 Class 1-Personal Firewall

A personal firewall is defined as a software service running in an operating system that provides simple firewall capability for a personal computer.

As the number of permanent Internet connections (as opposed to dial-up connections) has grown, the use of personal firewalls has increased.

Although designed to protect a single personal computer, a personal firewall can also protect a small network if the computer on which it is installed is sharing its connection to the Internet with other computers on the internal network. However, a personal firewall has limited performance and will degrade the performance of the personal computer on which it is installed.

The protection mechanisms are usually less effective than a dedicated firewall solution because they are usually restricted to blocking IP and port addresses, although in general a lower level of protection is needed on a personal computer.

Personal firewalls may come free-of-cost in an operating system or at a very low cost. They are suitable for their intended purpose but should not be considered for use in an enterprise, even for small satellite offices, due to their restricted performance and functionality. They are, however, particularly suitable for mobile users on laptop computers.

The following table shows the features that may be available in personal firewalls; they vary tremendously in their capabilities and price. However, lack of a specific feature, especially on a laptop, might not be of great importance.

Table 5.1: Class 1-Personal Firewalls

Firewall Attribute	Value
Basic features supported	Most personal firewalls support static packet filters, NAT, and stateful inspection, while some support circuit-level inspection and/or application layer filtering
Configuration	Automatic (manual option also available)
Block or allow IP addresses	Yes
Block or allow protocol or port numbers	Yes
Block or allow incoming ICMP messages	Yes
Control outgoing access	Yes
Application protection	Possibly
Audible or visible alerts	Possibly
Log file of attacks	Possibly
Real-time alerts	Depends on the product
VPN support	Typically no
Remote management	Typically no
Manufacturer support	Varies widely (depends on the product)
High-availability option	No
Number of concurrent sessions	1 to 10
Modular upgradeability (hardware or software)	None to limited
Price range	Low (free in some cases)

Advantages

The advantages of personal firewalls include:

Inexpensive : When only a limited number of licenses are required, personal firewalls are an inexpensive option. A personal firewall is integrated into versions of Windows XP. Additional products that work with other versions of Windows or other operating systems are available for free or at limited cost.

Easy to configure : Personal firewall products tend to have basic workable out-of-the-box configurations with straightforward configuration options.

Disadvantages

The disadvantages of personal firewalls include:

Difficult to manage centrally : Personal firewalls need to be configured on every client, which adds to management overhead.

Only basic control : Configuration tends to be a combination of static packet filtering and permission-based blocking of applications only.

Performance limitations :Personal firewalls are designed to protect single personal computers. Using them on a personal computer that serves as a router for a small network will lead to degraded performance.

5.2.2.2 Class 2-Router Firewall

Routers usually support one or more of the firewall features discussed previously; they can be subdivided into low-end devices designed for Internet connections and high-end traditional routers. The low-end routers provide basic firewall features for blocking and allowing specific IP addresses and port numbers and use NAT to hide interior IP addresses. They often provide the firewall feature as standard, optimized to block intrusions from the Internet, and while they need no configuration, they can be refined with further configuration.

High-end routers can be configured to tighten up access by barring the more obvious intrusions, such as pings, and by implementing other IP address and port restrictions through the use of ACLs. Additional firewall features may be available that provide stateful packet filtering in some routers. In high-end routers, the firewall capability is similar to that of a hardware firewall device, at a lower cost but also with lower throughput.

Table 5.2 Class 2-Router Firewall

Firewall Attribute	Value
Basic features supported	Most router firewalls support static packet filters. Lower-end routers typically support NAT. Higher-end routers may support stateful inspection and/or application layer filtering
Configuration	Typically automatic on lower-end routers (with manual options). Often manual on higher-end routers
Block or allow IP addresses	Yes
Block or allow protocol/port numbers	Yes
Block or allow incoming ICMP messages	Yes
Control outgoing access	Yes
Application protection	Possibly
Audible or visible alerts	Typically
Log file of attacks	In many cases
Real-time alerts	In many cases
VPN Support	Often in lower-end routers, not as common in higher-end routers. Separate dedicated devices or servers for this task are available
Remote management	Yes
Manufacturer support	Typically limited in lower-end routers and good in higher-end routers
High-availability option available	Low-end: no High-end: yes
Number of concurrent sessions	10 - 1,000
Modular upgradeability (hardware or software)	Low-end: no High-end: limited
Price range	Low to high

Advantages

The advantages of router firewalls include:

Low cost solution : Activation of an existing router firewall feature may not add any cost to the price of the router, and requires no additional hardware.

Configuration can be consolidated : Router firewall configuration can be accomplished when the router is configured for normal operations, thereby minimizing the management effort. This solution is particularly suitable for satellite branch offices, since network hardware and manageability are simplified.

Investment protection : Router firewall configuration and management is familiar to the operations staff and no retraining is required. Network cabling is simplified because no additional hardware is installed, which also simplifies network management.

Disadvantages

The disadvantages of router firewalls include:

Investment protection : Router firewall configuration and management is familiar to the operations staff and no retraining is required. Network cabling is simplified because no additional hardware is installed, which also simplifies network management.

Only basic control : Configuration tends to be a combination of static packet filtering and permission-based blocking of applications only.

Performance impact : Using a router as a firewall detracts from the performance of the router and slows the routing function, which is its primary task.

Log file performance : Use of a log file to catch unusual activities can seriously reduce performance of the router, especially when it is already under attack

5.2.2.3 Class 3-Low-end Hardware Firewall

At the low end of the hardware firewall market are Plug and Play units requiring little or no configuration. These devices often incorporate switch and/or VPN functionality.

Low-end hardware firewalls are suitable for small businesses and internal use in larger organizations. They generally offer static filtering capabilities and basic remote management functionality. Devices from larger manufacturers may run the same software as their higher-end counterparts, providing an upgrade path if you require one.

Table 5.3 Class 3-Low-End Hardware Firewall

Firewall Attribute	Value
Basic features supported	Most low-end hardware firewalls support static packet filters and NAT. May support stateful inspection and/or application layer filtering
Configuration	Automatic (manual option also available)
Block or allow IP addresses	Yes
Block or allow protocol/port numbers	Yes
Block or allow incoming ICMP messages	Yes
Control outgoing access	Yes
Application protection	Typically not
Audible or visible alerts	Typically not
Log file of attacks	Typically not
Real-time alerts	Typically not
VPN Support	Sometimes
Remote management	Yes
Manufacturer support	Limited
High-availability option available	Typically not
Number of concurrent sessions	> 10-7500
Modular upgradeability (hardware or software)	Limited
Price range	Low

Advantages

The advantages of low-end hardware firewalls include:

Low cost : Low-end firewalls can be purchased inexpensively.

Simple Configuration : Almost no configuration is required.

Disadvantages

The disadvantages of low-end hardware firewalls include:

Limited functionality : In general, low-end hardware firewalls only offer basic firewall functionality. They cannot be run in parallel for redundancy

Poor throughput :Low-end hardware firewalls are not designed to handle high-throughput connections, which may cause bottlenecks.

Limited manufacturer support : As these are low cost items, manufacturer support is usually limited to email and/or a Web site

Limited upgradeability : Usually there can be no hardware upgrades, though there are often periodic firmware upgrades available.

5.2.2.4 Class 4-High-end Hardware Firewall

At the high end of the hardware firewall market there are high performance, highly resilient products suitable for the enterprise or service provider. These usually offer the best protection without reducing the performance of the network.

Resilience can be achieved by adding a second firewall running as a hot standby unit that maintains the current table of connections through automatic stateful synchronization.

You should use firewalls in every network connected to the Internet because intrusion happens constantly; DoS attacks, theft, and data corruption are being attempted all the time. High-end hardware firewall units should be considered for deployment in central or head office locations.

Table 5.4: Class 4-High-End Hardware Firewall

Firewall Attribute	Value
Basic features supported	Most high-end hardware firewalls support static packet filters and NAT. They may support stateful inspection and/or application layer filtering
Configuration	Typically manual
Block or allow IP addresses	Yes
Block or allow protocol/port numbers	Yes
Block or allow Incoming ICMP messages	Yes
Control outgoing access	Yes
Application protection	Potentially
Audible or visible alerts	Yes
Log file of attacks	Yes
Real-time alerts	Yes
VPN support	Potentially
Remote management	Yes
Manufacturer support	Good
High-availability option available	Yes
Number of concurrent sessions	> 7500-500,000
Modular upgradeability (hardware or software)	Yes
Price range	High

Advantages

The advantages of high-end hardware firewalls include:

High performance : Hardware firewall products are designed for a single purpose and provide high levels of intrusion-blocking together with the least degradation of performance.

High availability : High-end hardware firewalls can be connected together for optimal availability and load balancing.

Modular systems : Both hardware and software can be upgraded for new requirements. Hardware upgrades may include additional Ethernet ports, while software upgrades may include detection of new methods of intrusion.

Remote management : High-end hardware firewalls offer better remote management functionality than their low-end counterparts.

Application layer filtering : Unlike their low-end counterparts which usually only filter at Layer 3 and perhaps Layer 4 of the OSI model, high-end hardware firewalls provide filtering at Layers 5 through 7 for well-known applications.

Disadvantages

The disadvantages of high-end hardware firewalls include:

High cost : High-end hardware firewalls tend to be expensive. Although they can be purchased for as little as \$100, the cost is much higher for an enterprise firewall and is often based on the number of concurrent sessions, throughput, and availability requirements.

Complex configuration and management : Because this class of firewalls has much greater capability than low-end firewalls, it is also more complex to configure and manage

5.2.2.5 Class 5-High-end Server Firewall

High-end server firewalls add firewall capability to a high-end server, providing robust fast protection on standard hardware and software systems. The benefit of this approach is the use of familiar hardware or software. This provides a reduced number of inventory items, simplified training and management, reliability, and expandability.

Many of the high-end hardware firewall products are implemented on industry standard hardware platforms with industry standard operating systems running on them (but hidden from view) and therefore have little difference, technically and in performance from a server firewall.

However, because the operating system is still visible, the server firewall feature can be upgraded and made more resilient by techniques such as clustering.

Because the server firewall is a server running a commonly used operating system, additional software, features, and functionality can be added to the firewall from a variety of vendors (not just one vendor, which is the case with the hardware firewall). Familiarity with the operating system can also lead to more effective firewall protection, because some of the other classes need considerable expertise for full and correct configuration.

This class is suitable where there is a high investment in a particular hardware or software platform, as using the same platform for the firewall makes the management task simpler. The caching capability of this class can also be very effective.

Table 5.5: Class 5-High-End Server Firewall

Firewall Attribute	Value
Features supported	Most high-end server firewalls support static packet filters and NAT. They may also support stateful inspection and/or application layer filtering
Configuration	Typically manual
Block or allow IP addresses	Yes
Block or allow protocol/port numbers	Yes
Block or allow incoming ICMP messages	Yes
Control outgoing access	Yes
Application protection	Potentially
Audible/visible alerts	Yes
Log file of attacks	Yes
Real-time alerts	Yes
VPN support	Potentially
Remote management	Yes
Manufacturer support	Good
High-availability option available	Yes
Number of concurrent sessions	>50,000 (across multiple network segments)
Modular upgradeability (hardware or software)	Yes
Other	Commonly used operating system
Price range	High

Advantages

The advantages of server firewalls include:

High performance : When run on a suitably sized server, these firewalls can offer high levels of performance

Integration and consolidation of services : Server firewalls can make use of features in the operating system they run on. For example, firewall software that runs on the Microsoft Windows Server™ 2003 operating system can take advantage of the Network Load Balancing functionality built into the operating system.

Additionally, the firewall could also serve as a VPN server, again utilizing functionality in the Windows Server 2003 operating system.

Availability, resilience, and scalability : Because this firewall runs on standard personal computer hardware, it has all the availability, resilience, and scalability features of the personal computer platform on which it runs.

Disadvantages

The disadvantages of server firewalls include:

Requires high-end hardware : For high performance, most server firewall products require high-end hardware in terms of central processing unit (CPU), memory and network interfaces.

Susceptible to vulnerabilities : Because server firewall products run on well-known operating systems, they are susceptible to the vulnerabilities present in the operating system and other software running on the server. Although this is also the case for hardware firewalls, their operating systems are not usually as familiar to attackers as most server operating systems.

5.2.3 Hardware Requirements

The hardware requirements for a firewall are different for software-based and hardware-based firewalls, as follows:

5.2.3.1 Hardware-based firewall

These devices typically run specialized code on a custom-built hardware platform. These firewalls are typically scaled (and priced) based on the number of connections they can handle and the complexity of the software that is to be run.

5.2.3.2 Software-based firewalls

These are also configured based on the number of concurrent connections and the complexity of the firewall software. Calculators exist that can compute the processor speed, memory size, and disk space needed for a server based on the number of connections supported. You should take into account other software that may be running on the firewall server, such as load balancing and VPN software. Also, consider the methods for scaling the firewall both upward and outward. These methods include increasing the power of the system by adding additional processors, memory, and network cards, and also using multiple systems and load balancing to spread the firewall task across them. Some products take advantage of symmetrical multiprocessing (SMP) to boost performance. The Network Load Balancing service of Windows Server 2003 can offer fault tolerance, high availability, efficiency, and performance improvements for some software firewall products.

Table 5.6 Hardware Firewalls versus Software

	Speed	Security	Flexibility	Price
Software Firewalls	-	-	+	+
Hardware Firewalls	+	+	-	-

5.2.4 What are proxy servers and how do they work?

A proxy server (sometimes referred to as an application gateway or forwarder) is an application that mediates traffic between a protected network and the Internet.

Proxies are often used instead of router-based traffic controls, to prevent traffic from passing directly between networks.

Many proxies contain extra logging or support for user authentication. Since proxies must ``understand" the application protocol being used, they can also implement protocol specific security (e.g., an FTP proxy might be configurable to permit incoming FTP and block outgoing FTP).

Proxy servers are application specific. In order to support a new protocol via a proxy, a proxy must be developed for it. One popular set of proxy servers is the TIS Internet Firewall Toolkit (``FWTK") which includes proxies for Telnet, rlogin, FTP, X-Window, HTTP/Web, and NNTP/Usenet news. SOCKS is a generic proxy system that can be compiled into a client-side application to make it work through a firewall. Its advantage is that it's easy to use, but it doesn't support the addition of authentication hooks or protocol specific logging.

5.2.5 What are the critical resources in a firewall?

It's important to understand the critical resources of your firewall architecture, so when you do capacity planning, performance optimizations, etc., you know exactly what you need to do, and how much you need to do it in order to get the desired result.

What exactly the firewall's critical resources are tends to vary from site to site, depending on the sort of traffic that loads the system. Some people think they'll automatically be able to increase the data throughput of their firewall by putting in a box with a faster CPU, or another CPU, when this isn't necessarily the case. Potentially, this could be a large waste of money that doesn't do anything to solve the problem at hand or provide the expected scalability.

On busy systems, *memory* is extremely important. You have to have enough RAM to support every instance of every program necessary to service the load placed on that machine. Otherwise, the swapping will start and the productivity will stop.

Light swapping isn't usually much of a problem, but if a system's swap space begins to get busy, then it's usually time for more RAM. A system that's heavily swapping is often relatively easy to push over the edge in a denial-of-service attack, or simply fall behind in processing the load placed on it. This is where long email delays start.

Beyond the system's requirement for memory, it's useful to understand that different services use different system resources. So the configuration that you have for your system should be indicative of the kind of load you plan to service. A 700 MHz processor isn't going to do you much good if all you're doing is netnews and mail, and are trying to do it on an IDE disk with an ISA controller.

Table 5.7: Critical Resources for Firewall Services

Service	Critical Resource
Email	Disk I/O
Netnews	Disk I/O
Web	Host OS Socket Performance
IP Routing	Host OS Socket Performance
Web Cache	Host OS Socket Performance, Disk I/O

5.2.6 What is a DMZ, and why do we want one?

“DMZ” is an abbreviation for “demilitarized zone”. In the context of firewalls, this refers to a part of the network that is neither part of the internal network nor directly part of the Internet. Typically, this is the area between your Internet access router and your bastion host, though it can be between any two policy-enforcing components of your architecture.

A DMZ can be created by putting access control lists on your access router. This minimizes the exposure of hosts on your external LAN by allowing only recognized and managed services on those hosts to be accessible by hosts on the Internet. Many commercial firewalls simply make a third interface off of the bastion host and label it the DMZ. The point is that the network is neither ``inside" nor ``outside".

For example, a web server running on NT might be vulnerable to a number of denial-of-service attacks against such services as RPC, NetBIOS and SMB.

These services are not required for the operation of a web server, so blocking TCP connections to ports 135, 137, 138, and 139 on that host will reduce the exposure to a denial-of-service attack. In fact, if you block everything but HTTP traffic to that host, an attacker will only have one service to attack.

This illustrates an important principle: never offer attackers more to work with than is absolutely necessary to support the services you want to offer the public.

5.2.7 How might we increase the security and scalability of my DMZ?

A common approach for an attacker is to break into a host that's vulnerable to attack, and exploit trust relationships between the vulnerable host and more interesting targets. If you are running a number of services that have different levels of security, you might want to consider breaking your DMZ into several ``security zones". This can be done by having a number of different networks within the DMZ. For example, the access router could feed two ethernet, both protected by ACLs, and therefore in the DMZ.

On one of the ethernet, you might have hosts whose purpose is to service your organization's need for Internet connectivity. These will likely relay mail, news, and host DNS. On the other ethernet could be your web server(s) and other hosts that provide services for the benefit of Internet users.

In many organizations, services for Internet users tend to be less carefully guarded and are more likely to be doing insecure things. (For example, in the case of a web server, unauthenticated and untrusted users might be running CGI or other executable programs. This might be reasonable for your web server, but brings with it a certain set of risks that need to be managed. It is likely these services are too risky for an organization to run them on a bastion host, where a slip-up can result in the complete failure of the security mechanisms.)

By putting hosts with similar levels of risk on networks together in the DMZ, you can help minimize the effect of a breakin at your site.

If someone breaks into your web server by exploiting some bug in your web server, they'll not be able to use it as a launching point to break into your private network if the web servers are on a separate LAN from the bastion hosts, and you don't have any trust relationships between the web server and bastion host.

Now, keep in mind that we're running ethernet here. If someone breaks into your web server, and your bastion host is on the same ethernet, an attacker can install a sniffer on your web server, and watch the traffic to and from your bastion host. This might reveal things that can be used to break into the bastion host and gain access to the internal network.

Splitting services up not only by host, but by network, and limiting the level of trust between hosts on those networks, you can greatly reduce the likelihood of a breakin on one host being used to break into the other. Succinctly stated: breaking into the web server in this case won't make it any easier to break into the bastion host.

You can also increase the scalability of your architecture by placing hosts on different networks. The fewer machines that there are to share the available bandwidth, the more bandwidth that each will get.

5.2.8 What is a 'single point of failure', and how to avoid having one?

An architecture whose security hinges upon one mechanism has a single point of failure. Software that runs bastion hosts has bugs. Applications have bugs. Software that controls routers has bugs. It makes sense to use all of these components to build a securely designed network, and to use them in redundant ways.

If your firewall architecture is a screened subnet, you have two packet filtering routers and a bastion host. Your Internet access router will not permit traffic from the Internet to get all the way into your private network. However, if you don't enforce that rule with any other mechanisms on the bastion host and/or choke router, only one component of your architecture needs to fail or be compromised in order to get inside. On the other hand, if you have a redundant rule on the bastion host, and again on the choke router, an attacker will need to defeat *three* mechanisms.

Further, if the bastion host or the choke router needs to invoke its rule to block outside access to the internal network, you might want to have it trigger an alarm of some sort, since you know that someone has gotten through your access router.

5.2.9 How to block all of the bad stuff?

For firewalls where the emphasis is on security instead of connectivity, you should consider blocking *everything* by default, and only specifically allowing what services you need on a case-by-case basis.

If you block everything, except a specific set of services, then you've already made your job much easier. Instead of having to worry about every security problem with everything product and service around, you only need to worry about every security problem with a specific set of services and products.

5.3 Various Attacks

5.3.1 What is source routed traffic and why is it a threat?

Normally, the route a packet takes from its source to its destination is determined by the routers between the source and destination. The packet itself only says where it wants to go (the destination address), and nothing about how it expects to get there.

There is an optional way for the sender of a packet (the source) to include information in the packet that tells the route the packet should take to get to its destination; thus the name "source routing". For a firewall, source routing is noteworthy, since an attacker can generate traffic claiming to be from a system "inside" the firewall.

In general, such traffic wouldn't route to the firewall properly, but with the source routing option, all the routers between the attacker's machine and the target will return traffic along the reverse path of the source route. Implementing such an attack is quite easy; so firewall builders should not discount it as unlikely to happen.

In practice, source routing is very little used. In fact, generally the main legitimate use is in debugging network problems or routing traffic over specific links for congestion control for specialized situations. When building a firewall, source routing should be blocked at some point. Most commercial routers incorporate the ability to block source routing specifically, and many versions of Unix that might be used to build firewall bastion hosts have the ability to disable or ignore source routed traffic.

5.3.2 What are ICMP redirects and redirect bombs?

An ICMP Redirect tells the recipient system to over-ride something in its routing table. It is legitimately used by routers to tell hosts that the host is using a non-optimal or defunct route to a particular destination, i.e. the host is sending it to the wrong router.

The wrong router sends the host back an ICMP Redirect packet that tells the host what the correct route should be. If you can forge ICMP Redirect packets, and if your target host pays attention to them, you can alter the routing tables on the host and possibly subvert the security of the host by causing traffic to flow via a path the network manager didn't intend. ICMP Redirects also may be employed for denial of service attacks, where a host is sent a route that loses its connectivity, or is sent an ICMP Network Unreachable packet telling it that it can no longer access a particular network. Many firewall builders screen ICMP traffic from their network, since it limits the ability of outsiders to ping hosts, or modify their routing tables.

Before you decide to completely block ICMP, you should be aware of how the TCP protocol does "Path MTU Discovery", to make certain that you don't break connectivity to other sites. If you can't safely block it everywhere, you can consider allowing selected types of ICMP to selected routing devices. If you don't block it, you should at least ensure that your routers and hosts don't respond to broadcast ping packets.

5.3.3 What about denial of service?

Denial of service is when someone decides to make your network or firewall useless by disrupting it, crashing it, jamming it, or flooding it. The problem with denial of service on the Internet is that it is impossible to prevent. The reason has to do with the distributed nature of the network: every network node is connected via other networks which in turn connect to other networks, etc. A firewall administrator or ISP only has control of a few of the local elements within reach. An attacker can always disrupt a connection "upstream" from where the victim controls it. In other words, if someone wanted to take a network off the air, they could do it either by taking the network off the air, or by taking the networks it connects to off the air, ad infinitum. There are many, many, ways someone can deny service, ranging from the complex to the brute-force.

If you are considering using Internet for a service which is absolutely time or mission critical, you should consider your fall-back position in the event that the network is down or damaged.

TCP/IP's UDP echo service is trivially abused to get two servers to flood a network segment with echo packets. You should consider commenting out unused entries in `/etc/inetd.conf` of Unix hosts, adding `no ip small-servers` to Cisco routers, or the equivalent for your components.

5.3.4 What are some common attacks, and how to protect system against them?

Each site is a little different from every other in terms of what attacks are likely to be used against it. Some recurring themes do arise, though.

5.3.4.1 SMTP Server Hijacking (Unauthorized Relaying)

This is where a spammer will take many thousands of copies of a message and send it to a huge list of email addresses. Because these lists are often so bad, and in order to increase the speed of operation for the spammer, many have resorted to simply sending all of their mail to an SMTP server that will take care of actually delivering the mail.

Of course, all of the bounces, spam complaints, hate mail, and bad PR come for the site that was used as a relay. There is a very real cost associated with this, mostly in paying people to clean up the mess afterward.

The Mail Abuse Prevention System Transport Security Initiative maintains a complete description of the problem, and how to configure about every mailer on the planet to protect against this attack.

5.3.4.2 Exploiting Bugs in Applications

Various versions of web servers, mail servers, and other Internet service software contain bugs that allow remote (Internet) users to do things ranging from gain control of the machine to making that application crash and just about everything in between.

The exposure to this risk can be reduced by running only necessary services, keeping up to date on patches, and using products that have been around a while.

5.3.4.3 Bugs in Operating Systems

Again, these are typically initiated by users remotely. Operating systems that are relatively new to IP networking tend to be more problematic, as more mature operating systems have had time to find and eliminate their bugs. An attacker can often make the target equipment continuously reboot, crash, lose the ability to talk to the network, or replace files on the machine.

Here, running as few operating system services as possible can help. Also, having a packet filter in front of the operating system can reduce the exposure to a large number of these types of attacks.

And, of course, choosing a stable operating system will help here as well. When selecting an OS, don't be fooled into believing that "the pricier, the better". Free operating systems are often much more robust than their commercial counterparts.

5.4 How Do We...

5.4.1 Do we really want to allow everything that our users ask for?

It's entirely possible that the answer is ``no". Each site has its own policies about what is and isn't needed, but it's important to remember that a large part of the job of being an organization's gatekeeper is *education* . Users want streaming video, real-time chat, and to be able to offer services to external customers that require interaction with live databases on the internal network.

That doesn't mean that any of these things can be done without presenting more risk to the organization than the supposed ``value" of heading down that road is worth. Most users don't want to put their organization at risk. They just read the trade rags, see advertisements, and they want to do those things, too. It's important to look into what it is that they really want to do, and to help them understand how they might be able to accomplish their real objective in a more secure manner.

You won't always be popular, and you might even find yourself being given direction to do something incredibly stupid, like ``just open up ports foo through bar". If that happens, don't worry about it. It would be wise to keep all of your exchanges on such an event so that when a 12-year-old script kiddie breaks in, you'll at least be able to separate yourself from the whole mess.

5.4.2 How do we make Web/HTTP work through my firewall?

There are three ways to do it.

1. Allow ``established" connections out via a router, if you are using screening routers.
2. Use a web client that supports SOCKS, and run SOCKS on your bastion host.

3. Run some kind of proxy-capable web server on the bastion host. Some options include Squid, Apache, Netscape Proxy, and *http-gw* from the TIS firewall toolkit. Most of these can also proxy other protocols (such as gopher and ftp), and can cache objects fetched, which will also typically result in a performance boost for the users, and more efficient use of your connection to the Internet. Essentially all web clients (Mozilla, Internet Explorer, Lynx, etc.) have proxy server support built directly into them.

5.4.3 How do we make SSL work through the firewall?

SSL is a protocol that allows secure connections across the Internet. Typically, SSL is used to protect HTTP traffic. However, other protocols (such as telnet) can run atop SSL.

Enabling SSL through your firewall can be done the same way that you would allow HTTP traffic, if it's HTTP that you're using SSL to secure, which is usually true. The only difference is that instead of using something that will simply relay HTTP, you'll need something that can tunnel SSL. This is a feature present on most web object caches.

5.4.4 How do we make DNS work with a firewall?

Some organizations want to hide DNS names from the outside. Many experts don't think hiding DNS names is worthwhile, but if site/corporate policy mandates hiding domain names, this is one approach that is known to work. Another reason you may have to hide domain names is if you have a non-standard addressing scheme on your internal network. In that case, you have no choice but to hide those addresses. Don't fool yourself into thinking that if your DNS names are hidden that it will slow an attacker down much if they break into your firewall. Information about what is on your network is too easily gleaned from the networking layer itself.

If you want an interesting demonstration of this, ping the subnet broadcast address on your LAN and then do an `arp -a`. Note also that hiding names in the DNS doesn't address the problem of host names "leaking" out in mail headers, news articles, etc.

This approach is one of many, and is useful for organizations that wish to hide their host names from the Internet. The success of this approach lies on the fact that DNS clients on a machine don't have to talk to a DNS server on that same machine. In other words, just because there's a DNS server on a machine, there's nothing wrong with (and there are often advantages to) redirecting that machine's DNS client activity to a DNS server on another machine.

First, you set up a DNS server on the bastion host that the outside world can talk to. You set this server up so that it claims to be authoritative for your domains. In fact, all this server knows is what you want the outside world to know; the names and addresses of your gateways, your wildcard MX records, and so forth. This is the "public" server.

Then, you set up a DNS server on an internal machine. This server also claims to be authoritative for your domains; unlike the public server, this one is telling the truth. This is your "normal" nameserver, into which you put all your "normal" DNS stuff. You also set this server up to forward queries that it can't resolve to the public server (using a "forwarders" line in `/etc/named.boot` on a Unix machine, for example).

Finally, you set up all your DNS clients (the `/etc/resolv.conf` file on a Unix box, for instance), including the ones on the machine with the public server, to use the internal server. This is the key. An internal client asking about an internal host asks the internal server, and gets an answer; an internal client asking about an external host asks the internal server, which asks the public server, which asks the Internet, and the answer is relayed back. A client on the public server works just the same way.

An external client, however, asking about an internal host gets back the ``restricted" answer from the public server.

This approach assumes that there's a packet filtering firewall between these two servers that will allow them to talk DNS to each other, but otherwise restricts DNS between other hosts.

Another trick that's useful in this scheme is to employ wildcard PTR records in your IN-ADDR.ARPA domains. These cause an address-to-name lookup for any of your non-public hosts to return something like ``unknown.YOUR.DOMAIN" rather than an error. This satisfies anonymous FTP sites like ftp.uu.net that insist on having a name for the machines they talk to. This may fail when talking to sites that do a DNS cross-check in which the host name is matched against its address and vice versa.

5.4.5 How do we make FTP work through my firewall?

Generally, making FTP work through the firewall is done either using a proxy server such as the firewall toolkit's ftp-gw or by permitting incoming connections to the network at a restricted port range, and otherwise restricting incoming connections using something like ``established" screening rules. The FTP client is then modified to bind the data port to a port within that range. This entails being able to modify the FTP client application on internal hosts.

In some cases, if FTP downloads are all you wish to support, you might want to consider declaring FTP a ``dead protocol" and letting your users download files via the Web instead. The user interface certainly is nicer, and it gets around the ugly callback port problem. If you choose the FTP-via-Web approach, your users will be unable to FTP files out, which, depending on what you are trying to accomplish, may be a problem.

A different approach is to use the FTP ``PASV" option to indicate that the remote FTP server should permit the client to initiate connections. The PASV approach assumes that the FTP server on the remote system supports that operation.

5.4.6 How do we make Telnet work through my firewall?

Telnet is generally supported either by using an application proxy such as the firewall toolkit's tn-gw, or by simply configuring a router to permit outgoing connections using something like the ``established" screening rules. Application proxies could be in the form of a standalone proxy running on the bastion host, or in the form of a SOCKS server and a modified client.

5.4.7 How do we make Finger and whois work through my firewall?

Many firewall admins permit connections to the finger port from only trusted machines, which can issue finger requests in the form of: finger user@host.domain@firewall. This approach only works with the standard Unix version of finger. Controlling access to services and restricting them to specific machines is managed using either tcp_wrappers or netacl from the firewall toolkit. This approach will not work on all systems, since some finger servers do not permit user@host@host fingering.

Many sites block inbound finger requests for a variety of reasons, foremost being past security bugs in the finger server (the Morris internet worm made these bugs famous) and the risk of proprietary or sensitive information being revealed in user's finger information. In general, however, if your users are accustomed to putting proprietary or sensitive information in their *.plan* files, you have a more serious security problem than just a firewall can solve.

5.4.8 How do we make gopher, archie, and other services work through my firewall?

The majority of firewall administrators choose to support gopher and archie through web proxies, instead of directly. Proxies such as the firewall toolkit's http-gw convert gopher/gopher+ queries into HTML and vice versa. For supporting archie and other queries, many sites rely on Internet-based Web-to-archie servers, such as ArchiePlex. The Web's tendency to make everything on the Internet look like a web service is both a blessing and a curse.

There are many new services constantly cropping up. Often they are misdesigned or are not designed with security in mind, and their designers will cheerfully tell you if you want to use them you need to let port xxx through your router. Unfortunately, not everyone can do that, and so a number of interesting new toys are difficult to use for people behind firewalls. Things like RealAudio, which require direct UDP access, are particularly egregious examples. The thing to bear in mind if you find yourself faced with one of these problems is to find out as much as you can about the security risks that the service may present, before you just allow it through. It's quite possible the service has no security implications. It's equally possible that it has undiscovered holes you could drive a truck through.

5.4.9 How do we make RealAudio work through our firewall?

RealNetworks maintains some information about how to get RealAudio working through your firewall. It would be unwise to make *any* changes to your firewall without understanding what the changes will do, exactly, and knowing what risks the new changes will bring with them.

5.4.10 How Do we Make IP Multicast Work With our Firewall?

IP multicast is a means of getting IP traffic from one host to a set of hosts without using broadcasting; that is, instead of every host getting the traffic, only those that want it will get it, without each having to maintain a separate connection to the server. IP unicast is where one host talks to another, multicast is where one host talks to a set of hosts, and broadcast is where one host talks to all hosts.

The public Internet has a multicast backbone ("MBone") where users can engage in multicast traffic exchange. Common uses for the MBone are streams of IETF meetings and similar such interaction. Getting one's own network connected to the MBone will require that the upstream provider route multicast traffic to and from your network. Additionally, your internal network will have to support multicast routing.

The role of the firewall in multicast routing, conceptually, is no different from its role in other traffic routing. That is, a policy that identifies which multicast groups are and aren't allowed must be defined and then a system of allowing that traffic according to policy must be devised. Great detail on how exactly to do this is beyond the scope of this document. Fortunately, RFC 2588 discusses the subject in more detail. Unless your firewall product supports some means of selective multicast forwarding or you have the ability to put it in yourself, you might find forwarding multicast traffic in a way consistent with your security policy to be a bigger headache than it's worth.

5.5 USEFUL KNOWLEDGE

5.5.1 What is a port?

A "port" is "virtual slot" in your TCP and UDP stack that is used to map a connection between two hosts.

Also between the TCP/UDP layer and the actual applications running on the hosts. They are numbered 0-65535, with the range 0-1023 being marked as ``reserved" or ``privileged", and the rest (1024-65535) as ``dynamic" or ``unprivileged".

Ports in the range 0-1023 are almost always server ports. Ports in the range 1024-65535 are usually dynamic ports (i.e., opened dynamically when you connect to a server port). However, *any* port may be used as a server port, and *any* port may be used as an ``outgoing" port.

5.5.2 How do we know which application uses what port?

There are several lists outlining the ``reserved" and ``well known" ports, as well as ``commonly used" ports, and the best one is: <ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers> . For those of you still reading RFC 1700 to find out what port number does what, STOP DOING IT. It is horribly out of date, and it won't be less so tomorrow. Now, as for trusting this information: These lists do not, in any way, constitute any kind of holy bible on which ports do what.

5.5.3 What are LISTENING ports?

Suppose you did ``netstat -a" on your machine and ports 1025 and 1030 showed up as LISTENing. What do they do?

Right, let's take a look in the assigned port numbers list.

```
blackjack    1025/tcp  network blackjack
iad1        1030/tcp  BBN IAD
```

Wait, what's happening? Has my workstation stolen my VISA number and decided to go play blackjack with some rogue server on the internet? And what's that software that BBN has installed?

This is NOT where you start panicking and send mail to the firewalls list. In fact, this question has been asked maybe a dozen times during the past six months, and every time it's been answered. Not that THAT keeps people from asking the same question again. If you are asking this question, you are most likely using a windows box. The ports you are seeing are (most likely) two listening ports that the RPC subsystem opens when it starts up.

This is an example of where dynamically assigned ports may be used by server processes. Applications using RPC will later on connect to port 135 (the netbios ``portmapper") to query where to find some RPC service, and get an answer back saying that that particular service may be contacted on port 1025.

Now, how do we know this, since there's no ``list" describing these ports? Simple: There's no substitute for experience. And using the mailing list search engines also helps a hell of a lot.

5.5.4 How do we determine what service the port is for?

Since it is impossible to learn what port does what by looking in a list, how do i do it?

The old hands-on way of doing it is by shutting down nearly every service/daemon running on your machine, doing `netstat -a` and taking note of what ports are open. There shouldn't be very many listening ones. Then you start turning all the services on, one by one, and take note of what new ports show up in your netstat output.

Another way, that needs more guess work, is simply telnetting to the ports and see what comes out. If nothing comes out, try typing some gibberish and slamming Enter a few times, and see if something turns up. If you get binary garble, or nothing at all, this obviously won't help you.

However, this will only tell you what listening ports are used. It won't tell you about dynamically opened ports that may be opened later on by these applications.

There are a few applications that might help you track down the ports used.

On Unix systems, there's a nice utility called `lsof` that comes preinstalled on many systems. It will show you all open port numbers and the names of the applications that are using them. This means that it might show you a lot of locally opened files aswell as TCP/IP sockets. Read the help text.

On windows systems, nothing comes preinstalled to assist you in this task. (What's new?) There's a utility called ``Inzider'' which installs itself inside the windows sockets layer and dynamically remembers which process opens which port.

5.5.5 What ports are safe to pass through a firewall?

The security of a ``port'' depends on what application you'll reach through that port. A common misconception is that ports 25 (SMTP) and 80 (HTTP) are safe to pass through a firewall. *meep* WRONG. Just because everyone is doing it doesn't mean that it is safe.

Again, the security of a port depends on what application you'll reach through that port.

If you're running a well-written web server, that is designed from the ground up to be secure, you can probably feel reasonably assured that it's safe to let outside people access it through port 80. Otherwise, you CAN'T.

The problem here is not in the network layer. It's in how the application processes the data that it receives. This data may be received through port 80, port 666, a serial line, floppy or through singing telegram. If the application is not safe, it does not matter how the data gets to it. The application data is where the real danger lies.

If you are interested in the security of your application, go subscribe to bugtraq or try searching their archives. This is more of an application security issue rather than a firewall security issue. One could argue that a firewall should stop all possible attacks, but with the number of new network protocols, NOT designed with security in mind, and networked applications, neither designed with security in mind, it becomes impossible for a firewall to protect against all data-driven attacks.

5.5.6 The behavior of FTP

Or, "Why do I have to open all ports above 1024 to my FTP server?"

FTP doesn't really look a whole lot like other applications from a networking perspective.

It keeps one listening port, port 21, which users connect to. All it does is let people log on, and establish ANOTHER connection to do actual data transfers. This second connection is usually on some port above 1024.

There are two modes, "active" (normal) and "passive" mode. This word describes the server's behaviour.

In active mode, the client (5.6.7.8) connects to port 21 on the server (1.2.3.4) and logs on. When file transfers are due, the client allocates a dynamic port above 1024, informs the server about which port it opened, and then the server opens a new connection to that port. This is the "active" role of the server: it actively establishes new connections to the client.

In passive mode, the connection to port 21 is the same. When file transfers are due, the SERVER allocates a dynamic port above 1024, informs the client about which port it opened, and then the CLIENT opens a new connection to that port. This is the "passive" role of the server: it waits for the client to establish the second (data) connection.

If your firewall doesn't inspect the application data of the FTP command connection, it won't know that it needs to dynamically open new ports above 1024.

On a side note: The traditional behaviour of FTP servers in active mode is to establish the data session FROM port 20, and to the dynamic port on the client. FTP servers are steering away from this behaviour somewhat due to the need to run as "root" on unix systems in order to be able to allocate ports below 1024. Running as "root" is not good for security, since if there's a bug in the software, the attacker would be able to compromise the entire machine. The same goes for running as "Administrator" or "SYSTEM" ("LocalSystem") on NT machines, although the low port problem does not apply on NT.

5.5.7 What software uses what FTP mode?

It is up to the client to decide what mode to use; the default mode when a new connection is opened is "active mode".

Most FTP clients come preconfigured to use active mode, but provide an option to use "passive" ("PASV") mode. An exception is the windows command line FTP client which only operates in active mode.

Web Browsers generally use passive mode when connecting via FTP, with a weird exception: MSIE 5 will use active FTP when FTP:ing in "File Explorer" mode and passive FTP when FTP:ing in "Web Page" mode. There is no reason whatsoever for this behaviour; my guess is that someone in Redmond with no knowledge of FTP decided that "Of course we'll use active mode when we're in file explorer mode, since that looks more active than a web page". Go figure.

5.5.8 Is our firewall trying to connect outside?

My firewall logs are telling me that my web server is trying to connect from port 80 to ports above 1024 on the outside. What is this?!

If you are seeing dropped packets from port 80 on your web server (or from port 25 on your mail server) to high ports on the outside, they usually DO NOT mean that your web server is trying to connect somewhere.

They are the result of the firewall timing out a connection, and seeing the server retransmitting old responses (or trying to close the connection) to the client. TCP connections always involve packets traveling in BOTH directions in the connection. If you are able to see the TCP flags in the dropped packets, you'll see that the ACK flag is set but not the SYN flag, meaning that this is actually not a new connection forming, but rather a response of a previously formed connection.

CHAPTER SIX

WIRELESS TECHNOLOGY

6. Overview of Wireless Technology

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections – without requiring network cabling. Wireless technologies use radio transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as WLANs and cell phones, to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. Wireless technology aims to provide users access to information anywhere – it allows mobility. Historically, the number one application for wireless has been mobile voice communication with cellular technology, that has been around since the early 1980s. Today, however, databased applications are beginning to burgeon. In this section, a brief overview of critical elements of wireless is presented: wireless networks, wireless devices, wireless standards, and wireless security issues.

6.1 Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range:

WWAN, WLAN, and WPAN. WWAN, representing wireless wide area networks, includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, Hyperlan, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and Infrared. All of these technologies are “tetherless” –they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum. (See Appendix A for a list of common wireless frequencies.) Because wireless network and technology are so diverse, we primarily focus on the WLAN and WPAN technologies. (WEB_4. 2004)

6.1.1 Wireless LANs

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device.

An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users even to “roam” within a building or between buildings.

6.1.2 Ad Hoc Networks

Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed ad hoc because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a system of mobile routers connected by wireless links to enable devices to communicate. In a Bluetooth network, mobile routers control the changing network topologies of these networks. The routers also control the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing protocol Bluetooth employs allows the routers to establish and maintain these shifting Networks

The mobile router is commonly integrated in a device such as a PDA (Figure 6-1). This mobile router, when configured, ensures that a remote, mobile device, such as a mobile phone, stays connected to the network. The router maintains the connection and controls the flow of communication. (Figure 6-1 also illustrates how with emerging technologies the mobile phone will be capable of connecting to the network, synchronizing the PDA address book, and downloading e-mail on an IEEE 802.11 WLAN all at the same time.)

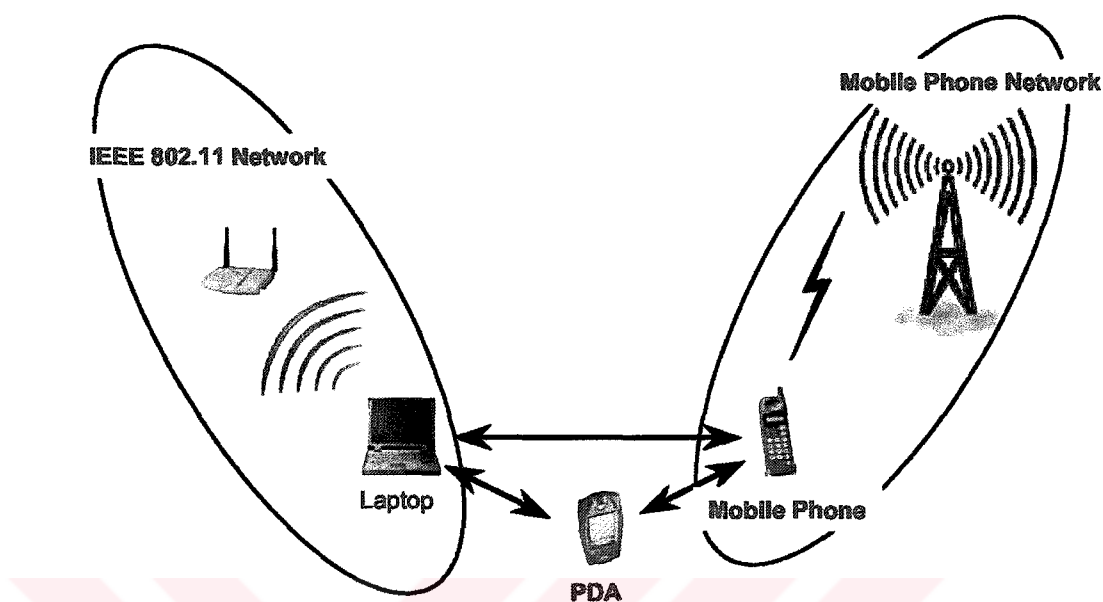


Figure 6.1. Ad Hoc Network

6.2 Wireless Devices

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. This document discusses the most commonly used wireless handheld devices such as text-messaging devices, PDAs, and Smart Phones.

Other devices include wireless e-mail devices with push technology, whereby e-mail gets delivered to the device without the user actually polling a Server (e.g., RIM's Blackberry device).

6.2.1 Personal Digital Assistants

PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. PDAs offer applications such as office productivity, database applications, address books, schedulers, and to-do lists, and they allow users to synchronize data between two PDAs and between a PDA and a personal computer. Newer versions allow users to download their e-mail and to connect to the Internet.

6.2.2 Smart Phones

Mobile wireless telephones, or cell phones, are telephones that have shortwave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. As with WLANs, the transmitter's span of coverage is called a cell. As the cell phone user moves from one cell to the next, the telephone connection is effectively passed from one local cell transmitter to the next. Today's cell phone is rapidly evolving to include integration with PDAs, thus providing users with increased wireless e-mail and Internet access. Mobile phones with information processing and data networking capabilities are called Smart Phones. This document addresses the risks introduced by the information processing and networking capabilities of Smart Phones.

6.2.3 Text-Messaging Devices

Security administrators may also encounter one-way and two-way text-messaging devices. These devices operate on a proprietary networking standard that disseminates e-mail to remote devices by accessing the corporate network. Text-messaging technology is designed to monitor a user's inbox for new e-mail and relay the mail to the user's wireless handheld via the Internet and wireless network.

6.3 Wireless Standards

Wireless, at its current relatively immature state, encompasses a variety of standards. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to communicate. The Advanced Mobile Phone Systems (AMPS) standard, which governed first generation mobile telephone devices, allowed devices from various manufacturers to work on wireless network infrastructure developed by other manufacturers.

The AMPS standard uses Frequency Division Multiple Access (FDMA) and requires a great deal of bandwidth while operating in the 824–829MHz range (similar to FM radios). Other telephony standards include IS-136, a Time Division Multiple Access (TDMA) standard, IS-95, a Code Division Multiple Access (CDMA) standard, and Global System for Mobile (GSM) – yet another TDMA standard. Many handheld devices (e.g., PDAs and cell phones) have followed the Wireless Application Protocol (WAP) standard, which provides for secure access to e-mail and the Internet. As briefly demonstrated, there are a plethora of wireless standards. All of these standards are different and offer varying levels of security features. For this document, the wireless standards discussion is limited to the IEEE 802.11 and the Bluetooth standard.

WLANs follow the IEEE 802.11 standards. Ad hoc networks follow proprietary techniques or are based on the Bluetooth standard, which was developed by a consortium of commercial companies making up the Bluetooth. Introductions to these are provided below.

6.3.1 IEEE 802.11

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. Mobile stations access the LAN while in motion, while portable stations are moved from location to location, but are only used while in a fixed physical location.

802.11 is the original WLAN standard, designed for 1Mbps to 2Mbps wireless transmissions. It was followed in 1999 by 802.11a, which established a high-speed WLAN standard for the 5GHz band and supported 54Mbps. Also completed in 1999 was the 802.11b standard, which operates in the 2.4 – 2.48GHz band and supports 11Mbps. The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications. (WEB_5. 2004)

Because the 802.11b standard has been so widely adopted, the security weaknesses in the standard have been exposed. These weaknesses will be discussed in Section 3.4.3.1.1. Another standard, 802.11g, still in draft, operates in the 2.4GHz waveband, where current WLAN products based on the 802.11b standard operate.

Two other important and related standards for WLANs are 802.1x and 802.11i. The 802.1x, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1x.

6.3.2 Bluetooth

Bluetooth has emerged as the primary ad hoc network standard. The Bluetooth standard is a computing and telecommunications industry specification that describes how mobile phones, computers, and PDAs should interconnect with each other, with home and business phones, and with computers using short-range wireless connections. Bluetooth network applications include wireless synchronization, e-mail/Internet/intranet access using local personal computer connections, hidden computing through automated applications and networking, and applications that can be used for such devices as hands-free headsets and car kits. The Bluetooth standard specifies wireless operation in the 2.45 Gigahertz (GHz) radio band and supports data rates up to 720kbps. It further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band. The IEEE 802.15 organization has derived a wireless personal area networking technology based on Bluetooth specifications v1.1

6.4 Wireless Security Threats and Risk Mitigation

- ☐ ☐ Errors and omissions
- ☐ ☐ Fraud and theft committed by authorized or unauthorized users of the system
- ☐ ☐ Employee sabotage
- ☐ ☐ Loss of physical and infrastructure support
- ☐ ☐ Malicious hackers
- ☐ ☐ Industrial espionage
- ☐ ☐ Malicious code
- ☐ ☐ Foreign government espionage
- ☐ ☐ Threats to personal privacy.

All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are fraud and theft, malicious hackers, malicious code, and industrial and foreign espionage. Theft is likely to occur with wireless devices due to their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, the former are more likely to carry out such acts. Since users of a system may know what resources a system has and the system security flaws, it is easier for them to commit fraud and theft. Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an organization (although users within an organization can be a threat as well). Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system. Industrial and foreign espionage involve gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the espionage threat stems from the relative ease in which eavesdropping can occur on radio transmissions.

These threats, if successful, place an organization's systems—and, more importantly, its data—at risk. Ensuring confidentiality, integrity, and network availability are (or should be) prime objectives of all government security policies and practices.

These are the areas of most concern for the ever-increasing use of wireless networks within government. Confidentiality is “the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.” The impact of unauthorized disclosure of confidential information can range from revealing private information about an individual to jeopardizing national security. Information that government organizations should keep confidential includes, for example, both sensitive but unclassified and classified information, proprietary information from companies and vendors, and any information about citizens that may be covered under the Privacy Act of 1974. Integrity is “the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Network availability is “the property of being accessible and usable upon demand by an authorized entity.”

The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

Risks in wireless networks are equal to the sum of the risk of operating a wired network (as in operating a network in general) plus the new risks introduced by weaknesses in wireless protocols. To mitigate these risks, organizations need to adopt security measures and practices that help bring their risks to a manageable level. They need, for example, to perform security assessments prior to implementation to determine the specific threats and vulnerabilities wireless networks will introduce in their environments.

In performing the assessment, they should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs of security measures, and technical requirements. Once the risk assessment is complete, the organization can begin planning and implementing the measures it will put in place to safeguard its systems and lower its security risks to a manageable level. The organization will need to reassess periodically the policies and measures it puts in place because computer technologies and malicious threats are continually changing. To date, the list below represents some of the more salient threats and vulnerabilities of wireless systems:

- ☐ ☐ All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- ☐ ☐ Malicious entities may gain unauthorized access to an organization's computer network through wireless connections, bypassing any firewall protections.
- ☐ ☐ Sensitive information that is not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- ☐ ☐ Denial of service (DoS) attacks may be directed at wireless connections or devices.
- ☐ ☐ Malicious entities may steal the identity of legitimate users and masquerade on internal or external corporate networks.
- ☐ ☐ Sensitive data may be corrupted during improper synchronization.
- ☐ ☐ Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements.
- ☐ ☐ Handheld devices are easily stolen and can reveal sensitive information.
- ☐ ☐ Data may be extracted without detection from improperly configured devices.
- ☐ ☐ Viruses or other malicious code may corrupt data on a wireless device and be introduced to a wired network connection.
- ☐ ☐ Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks and concealing their activity.

- Interlopers, from insider or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

6.5 Emerging Wireless Technologies

Originally, handheld devices had limited functionality because of size and power requirements. However, the technology is improving and handheld devices are becoming more feature-rich and portable. More significantly, the various wireless devices and their respective technologies are coalescing. The mobile phone, for instance, has increased functionality that now allows it to serve as a PDA as well as a phone.

Smart phones are merging mobile phone and PDA technologies to provide normal voice service and e-mail, text messaging, paging, web access, and voice recognition. Next-generation mobile phones, already on the market, are quickly incorporating PDA, IR, wireless Internet, e-mail, and GPS capabilities.

Manufacturers are combining standards as well, with the goal to provide a device capable of delivering multiple services. Other developments that will soon be on the market include GSM-based technologies such as General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS). These technologies will provide high data transmission rates and greater networking capabilities. However, each new development will present its own security risks, and government agencies must address these risks to ensure that critical assets remain protected.

CHAPTER SEVEN

WIRELESS LANs

7. Wireless LANs

This section provides a detailed overview of 802.11 WLAN technology. The section includes introductory material on the history of 802.11 and provides other technical information including 802.11 frequency ranges and data rates, network topologies, transmission ranges, and applications. It examines the security threats and vulnerabilities associated with WLANs and offers various means for reducing risks and securing WLAN environments. (WEB_6. 2004)

7.1 Wireless LAN Overview

WLAN technology and the WLAN industry date back to the mid-1980s when the Federal Communications Commission (FCC) first made available the radio frequency spectrum. During the 1980s and early 1990s, growth was relatively slow. Today, however, WLAN technology is experiencing tremendous growth. There are several reasons for the growth, but the key reason is because of the increased bandwidth of the IEEE 802.11b standard of WLAN technology. As an introduction to the 802.11 and WLAN technology, Table 7-1 provides some key characteristics at a glance.

Table 7.1. Key Characteristics of 802.11 Wireless LANs

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

7.1.1 Brief History

Motorola developed one of the first commercial WLAN systems with its Altair product. However, early WLAN technologies had several problems that prohibited its pervasive use. These LANs were expensive, provided low data rates, were prone to radio interference, and were designed mostly to proprietary RF (radio frequency) technologies. The Institute of Electrical and Electronics Engineers (IEEE) initiated the 802.11 project in 1990 with a scope “to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area.” In 1997, IEEE first approved the 802.11 international interoperability standard. Then, in 1999, the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards.

The goal was to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications, similar to what was done with the 802.3 Ethernet standard. The 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference.

This soon-to-be introduced technology will use the 5GHz frequency spectrum and can process data at up to 54Mbps. The direct descendent of 802.11a, IEEE's 802.11b, is the focus of this document.

Although this document focuses on the IEEE 802.11b WLAN standard, it is important to note that several other WLAN technologies and standards are available from which consumers may choose, including HiperLAN and HomeRF.

7.1.2 Frequency and Data Rates

IEEE developed the 802.11 standards to provide wireless networking technology like the wired Ethernet that has been available for many years. The popular IEEE 802.11b standard is the latest completed member of 802.11 WLAN family. The 802.11b standard operates in the unlicensed 2.4GHz–2.5GHz ISM (Industrial, Scientific, and Medical) frequency band using a direct sequence spread-spectrum technology. The ISM band has become popular for wireless communications because it is available worldwide. The 802.11b standard focuses on the MAC and PHY protocols for connectivity. The 802.11b WLAN technology permits transmission speeds of up to 11Mbps per second. This makes it considerably faster than the original IEEE 802.11 standard (that sends data at up to 2Mbps) and slightly faster than standard Ethernet.

7.1.3 Architecture

The IEEE 802.11b standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can

communicate. Hence, the standard defines two basic network topologies: the infrastructure network and the ad hoc network. The infrastructure network is meant to extend the range of the wired LAN to wireless cells. A laptop or other mobile device may move from cell to cell (from AP to AP) while maintaining access to the resources of the LAN. A cell is the area covered by an AP and is called a basic service set (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS). This first topology is useful for providing wireless coverage of building or campus areas.

By deploying multiple APs with overlapping coverage areas, broad network coverage can be achieved. WLAN technology can be used to replace wired LANs totally as well as to extend LAN infrastructure.

A WLAN environment has wireless client stations that use radio modems to communicate to an AP. The client stations are generally equipped with a wireless network interface card (NIC) that consists of the radio modem and the logic to interact with the client machine and software. An AP comprises essentially a radio modem on one side and a bridge to the wired backbone on the other. The AP, a stationary device that is part of the wired infrastructure, is analogous to a cell-site (base station) in cellular communications. All communications between the client stations and between clients and the wired network go through the AP. The basic topology of a WLAN is depicted in Figure 7-1.

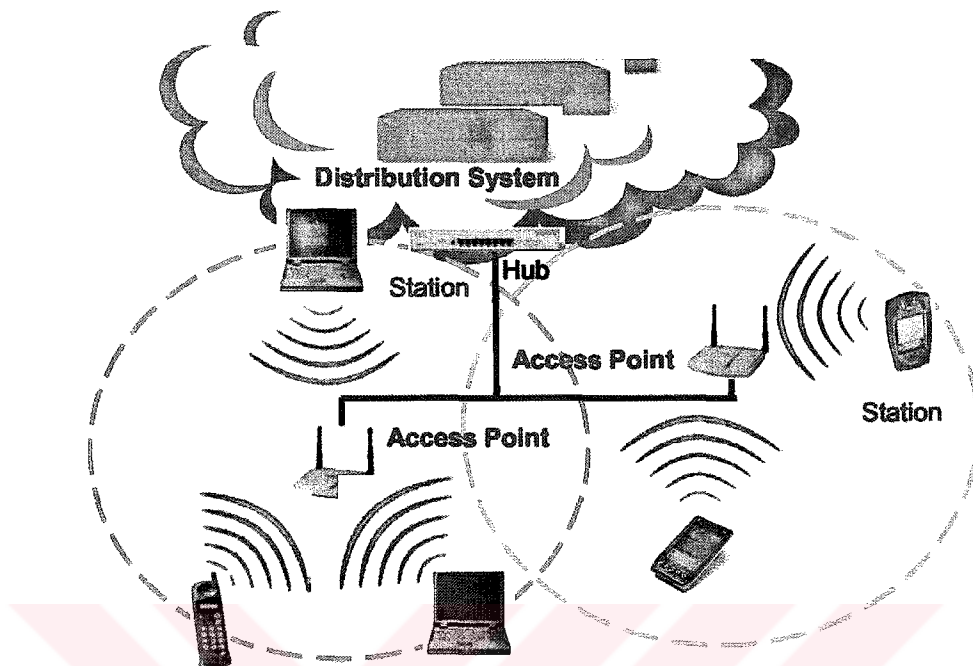


Figure 7.1. Fundamental 802.11b Wireless LAN Topology

Although most WLANs operate in the “infrastructure” mode and architecture described above, another topology is also possible.

This second topology, the ad hoc network, is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be internetworked without access to the wired LAN (infrastructure network). The interconnected devices in the ad hoc mode are referred to as an IBSS (independent basic service set). The ad hoc topology is depicted in Figure 7-2 below.

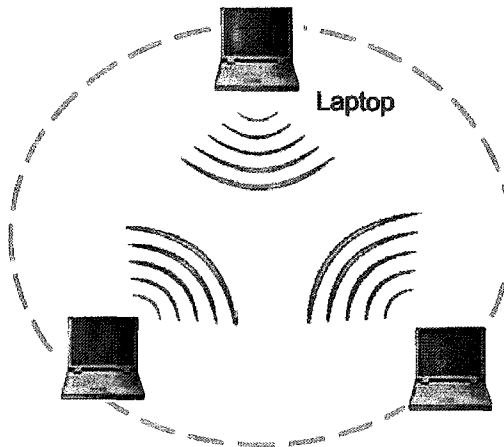


Figure 7.2. 802.11b Wireless LAN Ad hoc Topology

The ad hoc configuration is similar to a peer-to-peer office network in which no node is required to function as a server. As an ad hoc WLAN, laptops, desktops and other 802.11 devices can share files without the use of an AP.

7.1.4 Wireless LAN Components

A WLAN comprises two types of equipment: a wireless station and an access point. A station, or client, is typically a laptop or notebook personal computer (PC) with a wireless network interface card (NIC).

A WLAN client may also be a desktop or handheld device (e.g., PDA, or custom device such as a barcode scanner), or equipment within a kiosk, on a manufacturing floor, or other publicly accessed area. Wireless laptops and notebooks—"wireless enabled"—are identical to laptops and notebooks except that they use wireless NICs to connect to access points in the network.

The wireless NIC is commonly inserted in the client's Personal Computer Memory Card International Association (PCMCIA) slot or Universal Serial Bus (USB) port. The NICs use radio frequencies or infrared beams to establish connections to the WLAN.

The AP, which acts as a bridge between the wireless and wired networks, typically comprises a radio, a wired network interface such as 802.3, and bridging software. The AP functions as a base station for the wireless network, aggregating multiple wireless stations onto the wired network. (WEB_7. 2004)

7.1.5 Range

The reliable coverage range for 802.11b WLANs depends on several factors including data rate required and capacity, sources of RF interference, physical area and characteristics, power, connectivity, and antenna usage. Theoretical ranges are from 29 meters (for 11Mbps) in a closed office area to 485 meters (for 1Mbps) in an open area. However, through empirical analysis, the typical range for connectivity of 802.11b equipment is approximately 50 meters (about 163 ft.) indoors. With an omni-directional antenna outdoors, the connectivity can be increased to 400 meters. A range of 400 meters, nearly $\frac{1}{4}$ mile, makes WLAN ideal technology for many campus applications. It is important to recognize that special high-gain antennas can increase the range to several miles.

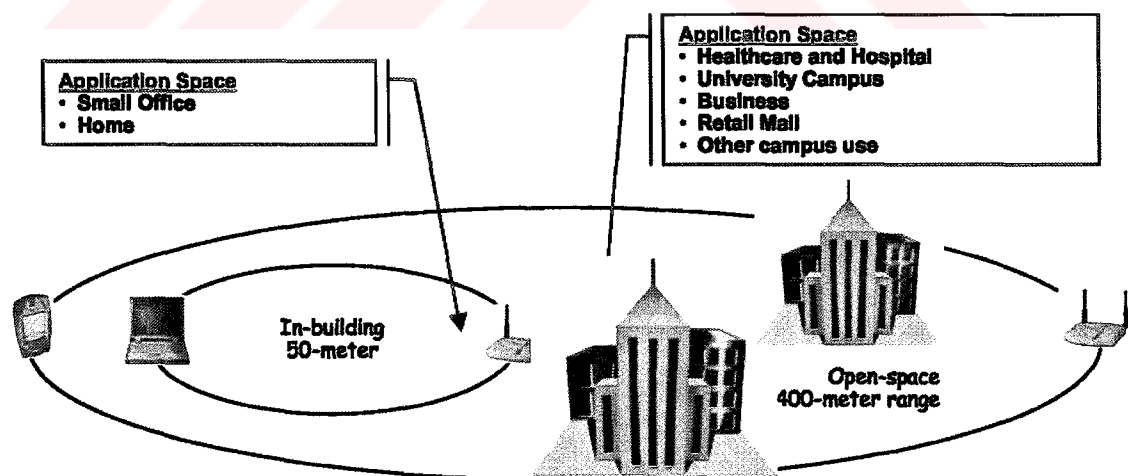


Figure 7.3. Typical Range of 802.11 WLAN

APs may also provide a “bridging” function. Bridging connects two or more networks together and allows them to communicate—to exchange network traffic. Bridging involves either a point-to-point or a multipoint configuration. In a point-to-point architecture, two LANs are connected to each other via the LANs’ respective APs. In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP. For example, if a computer on Subnet A needed to connect to computers on Subnets B, C, and D, Subnet A’s AP would connect to B, C, and D’s respective APs.

Enterprises may use bridging to connect LANs between different buildings on corporate campuses. Bridging AP devices are typically placed on top of buildings to achieve greater antenna reception. The typical distance over which one AP can be connected wirelessly to another by means of bridging is approximately 2 miles. This distance may vary depending on several factors including the specific receiver or transceiver being used. Figure illustrates point-to-point bridging between two LANs. In the example, wireless data is being transmitted from Laptop A to Laptop B, from one building to the next, using each building’s appropriately positioned AP. Laptop A connects to the closest AP within the building A. The receiving AP in building A then transmits the data (over the wired LAN) to the AP bridge located on the building’s roof. That AP bridge then transmits the data to the bridge on nearby building B. The building’s AP bridge then sends the data over its wired LAN to Laptop B.

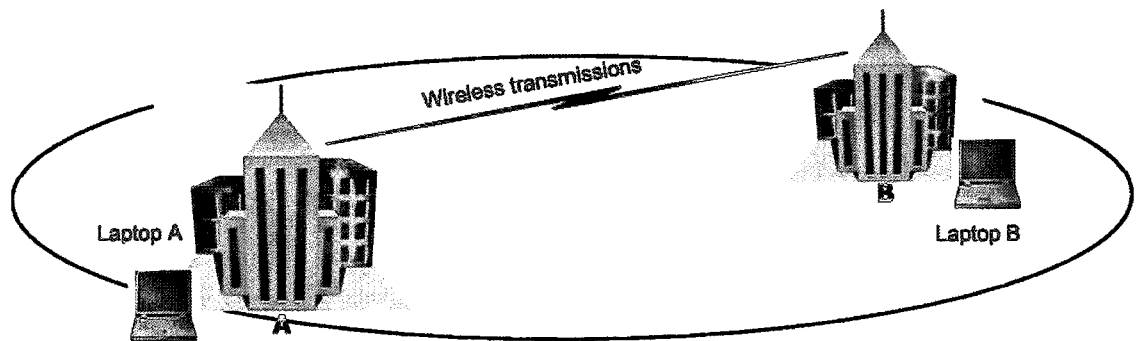


Figure 7.4. Access Point Bridging

7.2 Benefits

WLANs' "untethered" method of communication, making them very attractive today, can result both in increased efficiency and reduced costs. The efficiencies and cost savings are attractive for home and enterprise users.

WLANs offer four primary benefits to users:

- * **User Mobility**—Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.
- * **Rapid Installation**—The time required for installation is reduced because network connections can be made without moving or adding wires, or pulling them through walls or ceilings.
- * **Flexibility**—Enterprises can also enjoy the flexibility of installing and taking down WLANs in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, trade show, or standards meeting.

- * Scalability—WLAN network topologies can easily be configured to meet specific application and installation needs and to scale from small P2P networks to very large enterprise networks that enable roaming over a broad area.

Because of these fundamental benefits, the WLAN market has been increasing steadily over the past several years, and WLANs are still gaining in popularity. According to IDC, the number of mobile subscribers will surpass 500 million worldwide by 2002. IDC also posits that sales of WLAN technology will reach \$3.2 billion by 2005. WLANs are now becoming a viable alternative to traditional wired solutions. In fact, hospitals, universities, airports, hotels, and specialty shops are now offering WLAN access to the Internet.

7.3 Security of 802.11 Wireless LANS

This section helps the reader understand the built-in security features of 802.11b. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. The IEEE 802.11b specification identified several services to provide a secure operating environment. The security services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link-level data during wireless transmission between clients and access points. That is, WEP does not provide end-to-end security but only for the wireless portion of the connection. Security for the radiopath is depicted in Figure 7-5.

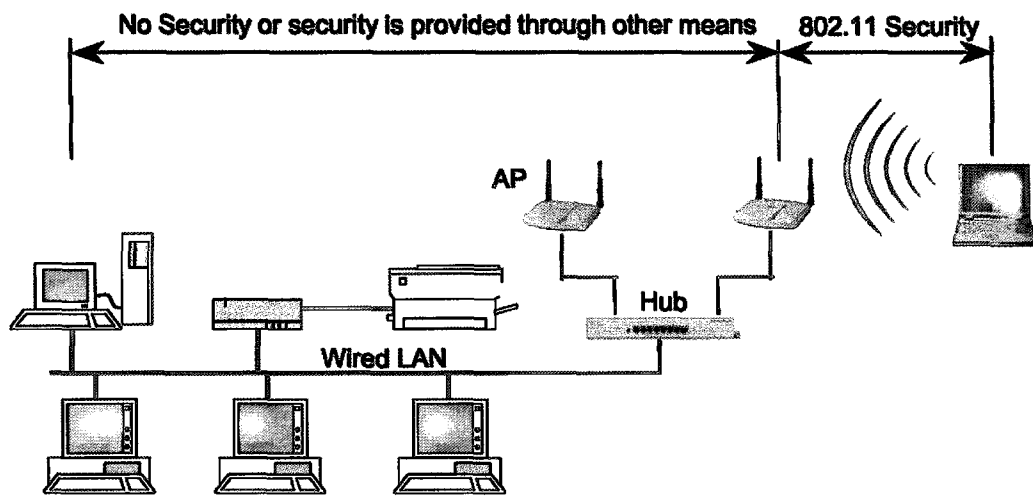


Figure 7.5. Wireless Security of 802.11b in Typical Network

7.3.1 Security of the WEP algorithm

7.3.1.1 The WEP mechanism

1-The WEP uses the RC4 stream cipher, a cryptographic algorithm, in order to generate a key stream. The key is shared between members on the WLAN.

2-The key is XORed with plaintext to produce ciphertext.

3-The process is reversed for decryption.

4-Additionally, a 24-bit initialization vector (IV) is generated and is appended to the shared key; WEP uses this combined key and IV to generate the RC4 key schedule.

WEP selects a new IV for every packet that points to a unique key.

WEP uses an Integrity Check (IC) field in the packet, in order to ensure that a packet has not been modified in transit.

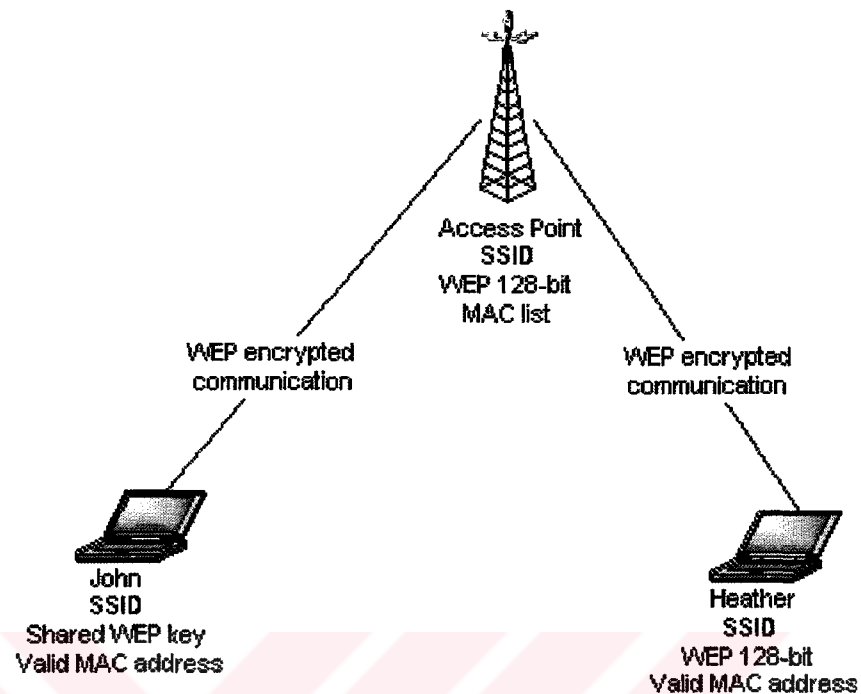


Figure 7.6 Basic WLAN Architecture with 128-bit key

7.3.1.2 WEP ENCRYPTION DESCRIBE

The Wired Equivalent Privacy protocol is used in 802.11 networks to protect link-level data during wireless transmission. It is described in detail in the 802.11 standard ; we reproduce a brief description to enable the following discussion of its properties.

WEP relies on a secret key _ shared between the communicating parties to protect the body of a transmitted frame of data. Encryption of a frame proceeds as follows:

Check Summing First, we compute an *integrity checksum* $c(M)$ on the message M . We concatenate the two to obtain a plaintext $P = (M, c(M))$, which will be used as input to the second stage. Note that $c(M)$, and thus P , does not depend on the key k .

Encryption: In the second stage, we encrypt the plaintext P derived above using RC4. We choose an initialization vector (IV) v . The RC4 algorithm generates a *keystream*—i.e., a long sequence of pseudorandom bytes—as a function of the (IV) v and the key k . This keystream is denoted by $RC4(v,k)$. Then we exclusive-or (XOR, denoted by \oplus) the plaintext with the keystream to obtain the ciphertext.

$$C = P \oplus RC4(v,k)$$

Transmission Finally we transmit IV and the ciphertext over the radio link

Symbolically, this may be represented as below

$$A \rightarrow B : v, (P \oplus RC4(v,k)) \text{ where } P = (M, c(M))$$

The format of the encrypted frame as also shown in Figure

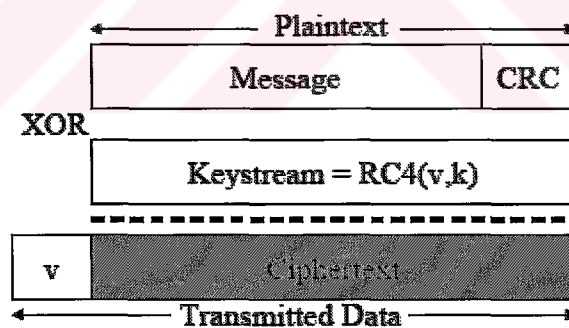


Figure 7.7 : Encrypted WEP Frame.

We will consistently use the term *message* (symbolically, M) to refer to the initial frame of data to be protected, the term *plaintext* (P) to refer to the concatenation of message and checksum as it is presented to the RC4 encryption algorithm, and the term *ciphertext* (C) to refer to the encryption of the plaintext as it is transmitted over the radio link.

To decrypt a frame protected by WEP, the recipient simply reverses the encryption process. First, he regenerates the keystream RC4 (v,k) and XORs it against the ciphertext to recover the initial plaintext

$$P' = C \oplus \text{RC4}(v,k) \Rightarrow (P \oplus \text{RC4}(v,k)) \oplus \text{RC4}(v,k) \Rightarrow P$$

Next, the recipient verifies the checksum on the decrypted plaintext P' by splitting it into the form (M' , c') , re-computing the checksum c (M') , and checking that it matches the received checksum c'. This ensures that only frames with a valid checksum will be accepted by the receiver.

7.3.2 Security Features of 802.11 Wireless LANS per the Standard

The three basic security services defined by IEEE for the WLAN environment are as follows:

- * **Authentication**—A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This is to provide access control to the network through denying access to client stations that cannot authenticate properly. This service addresses the question, “Are only authorized persons allowed to gain access to my network?”
- * **Confidentiality**—Confidentiality, or privacy, was a second goal of WEP. It was developed to provide “privacy achieved by a wired network.” The intent was to prevent information compromise from casual eavesdropping (passive attack). This service, in general, addresses the question, “Are only authorized persons allowed to view my data?”
- * **Integrity**—Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack.

This service addresses the question, “Is the data coming into or exiting the network trustworthy – has it been tampered with?”

It is important to note that the standard did not address other security services such as audit, authorization, and non-repudiation. These three security services offered by 802.11 are described in greater detail below.

7.3.2.1 Authentication

The IEEE 802.11b specification defines two means to validate wireless users attempting to gain access to the wired network, as depicted previously. One means is based on cryptography and the other is not. For the non-cryptographic approach, there are essentially two different ways to identify a wireless client attempting to join a network. However, both of these approaches are identity-based verification mechanisms. The wireless stations requesting access simply respond with the Service Set Identifier (SSID) of the wireless network—there is no true “authentication.” The two ways are referred to as Open System authentication and Closed System authentication. A taxonomy of the techniques for 802.11b is depicted in Figure 7.8.

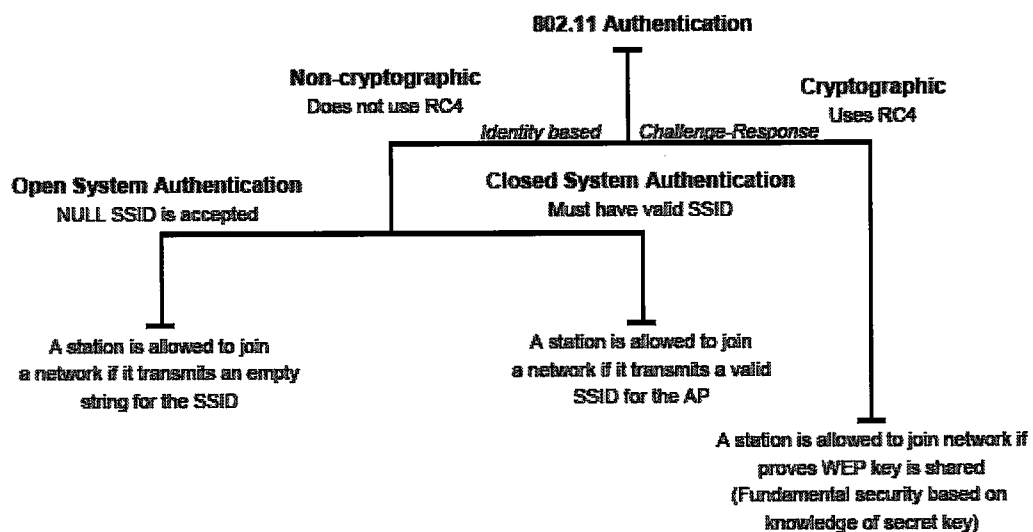


Figure 7.8: Taxonomy of 802.11b Authentication Techniques

With Open System, a client is authenticated if it simply responds with an empty string for the SSID (Service Set Identifier)—hence, the name “NULL authentication.” With the second method, Closed Authentication, wireless clients must respond with the actual SSID of the wireless network. That is, a client is allowed access if it responds with the correct 0-byte to 32-byte string identifying the BSS of the wireless network. Again, this primitive type of authentication is only an identification scheme.

Practically speaking, neither of these two schemes offers robust security against unauthorized access. To reiterate, both Open and Closed Authentication schemes are highly vulnerable to attacks—against even the most novice adversaries—and without enhancements, they practically invite security incidents.

Shared key authentication is a cryptographic technique for authentication. It is a simple “challenge-response” scheme based on whether a client has knowledge of a shared secret. In this scheme, as depicted in Figure 7-9, a random challenge is generated by the access point and sent to the wireless client.

The client, using a cryptographic key (WEP key) that is shared with the AP, encrypts the challenge (or “nonce,” as it is called in security vernacular) and returns the result to the AP. The AP decrypts the result computed by the client and allows access only if the decrypted value is the same as the random challenge transmitted. The algorithm used in the cryptographic computation is the RC4 stream cipher developed by Ron Rivest of MIT. It should be noted that the authentication method just described is a rudimentary cryptographic technique, and it does not provide mutual authentication. That is, the client does not authenticate the AP and therefore there is no assurance that a client is communicating with a legitimate AP, and wireless network. It is also worth noting that simple unilateral challenge-response schemes have long been known to be weak. They suffer from numerous attacks including the infamous “man-in-the-middle” attack.

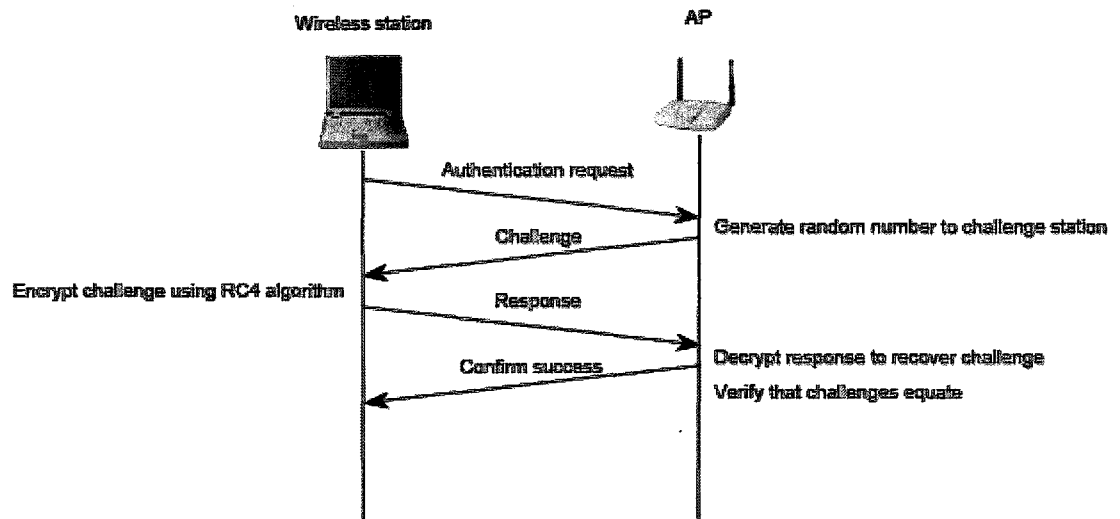


Figure 7.9. Shared-key Authentication Message Flow

7.3.2.2 Privacy

The 802.11b standard supports privacy (confidentiality) through the use of cryptographic techniques for the wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric-key, stream cipher algorithm to generate a pseudo random data sequence. This “keystream” is simply added modulo 2 (exclusive-ORed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link.

WEP is applied to all data above the 802.11b WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP).

The WEP supports cryptographic keys sizes from 40-bits to 104-bits. The 104-bit WEP key, for instance, with a 24-bit IV becomes a 128-bit RC4 key. In general, increasing the key size increases the security of a cryptographic technique.

Research has shown that key sizes of greater than 80-bits make brute-force cryptanalysis (codebreaking) an impossible task. For 80-bit keys, the number of possible keys—a key space of more than 10^{24} —exceeds contemporary computing power. However, in practice, most WLAN deployments rely on 40-bit keys. Moreover, recent attacks have shown that the WEP approach for privacy is, unfortunately, vulnerable to certain attacks regardless of key size

The WEP privacy is illustrated conceptually in Figure 7.10.

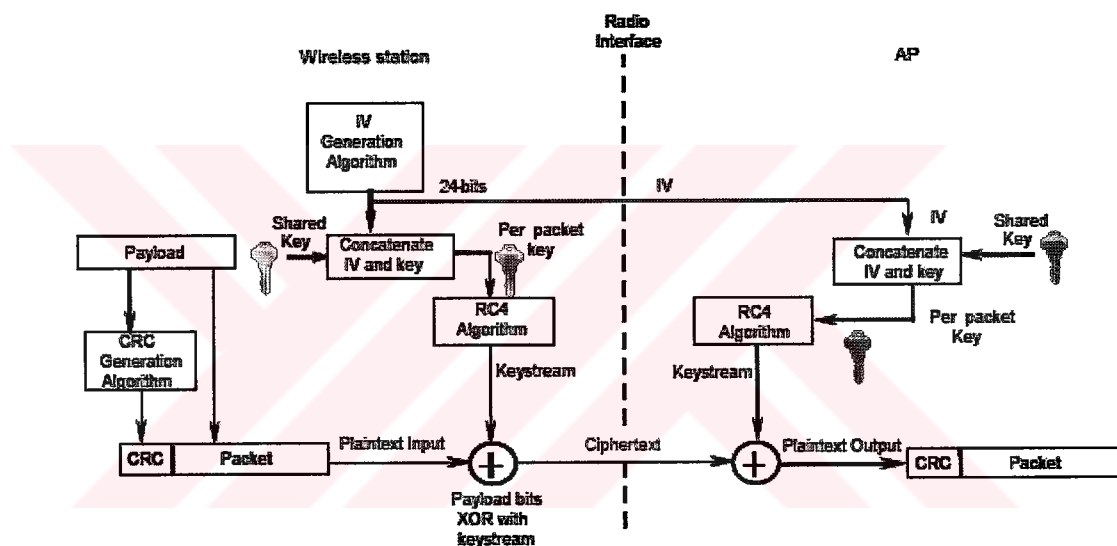


Figure 7.10. WEP Privacy Using RC4 Algorithm

7.3.2.3 Integrity

The IEEE 802.11b specification also outlines a means to provide data integrity for messages transmitted between wireless clients and access points. This security service was designed to reject any messages that had been changed by an active adversary “in the middle.”

This technique uses a simple encrypted Cyclic Redundancy Check (CRC) approach. As depicted in the diagram above, a CRC-32, or frame check sequence, is computed on each payload prior to transmission. The integrity-sealed packet is then encrypted using the RC4 key stream to provide the ciphertext message. On the receiving end, decryption is performed and the CRC is recomputed on the message that is received. The CRC computed at the receiving end is compared with the one computed with the original message. If the CRCs do not equal, that is, “received in error,” this would indicate an integrity violation (an active message spoofer), and the packet would be discarded. As with the privacy service, unfortunately, the 802.11b integrity is vulnerable to certain attacks regardless of key size.

The IEEE 802.11b specification does not, unfortunately, identify any means for key management (life cycle handling of cryptographic keys and related material). Therefore, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material is left to those deploying WLANs. Again, key management (probably the most critical aspect of a cryptographic system) for 802.11b is left largely as an exercise for the users of the 802.11b network (perhaps, individuals not totally cognizant of its importance). As a result, many vulnerabilities can be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns). Additionally, because key management is poor for 802.11b, WEP-secured WLANs suffer from the inability to scale. In other words, even if an enterprise recognizes the need to change keys often and to make them random, the task is formidable in a large WLAN environment. For example, a large campus may have as many as 15,000 Aps.

Generating, distributing, loading, and managing keys for an environment of this size is a most significant challenge.

7.3.3 Problems with the IEEE 802.11b Standard Security

This section discusses some known vulnerabilities in the standardized security of the 802.11b WLAN standard. As mentioned above, the WEP protocol is used in 802.11-based WLANs. WEP in turn uses a RC4 cryptographic algorithm with a variable length key to protect traffic. Again, the 802.11 standard supports WEP cryptographic keys of 40-bits. However, some vendors have implemented products with keys to 104-bits, plus the addition of a 24-bit IV. It is worthy to note that keys are often based on passwords that are chosen by users; this typically reduces the effective key size.

Several groups of computer security specialists have discovered security problems that let malicious users compromise the security of WLANs. These include passive attacks to decrypt traffic based on statistical analysis, active attacks to inject new traffic from unauthorized mobile stations (i.e., based on known plaintext), active attacks to decrypt traffic (i.e., based on tricking the access point), and dictionary-building attacks. The dictionary building attack is possible after analyzing a full day's traffic. Because significant attention is now on the security of 802.11, more attacks are likely to be discovered. (WEB_8. 2004)

There are several problems with WEP, including the following:

1. The use of static WEP keys—many users in a wireless network potentially sharing the identical key for long periods of time, is a well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key. Moreover, since every station uses the same key, a large amount of traffic may be rapidly available to an eavesdropper for analytic attacks, such as 2 and 3 below.

2. The initialization vector (IV) in WEP, is a 24-bit field sent in the clear text portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes. Reuse of the same IV produces identical key streams for the protection of data, and the short IV guarantees that they will repeat after a relatively short time in a busy network.

Moreover, the 802.11 standard does not specify how the IVs are set or changed, and individual wireless NICs from the same vendor may all generate the same IV sequences, or some wireless NICs may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the ciphertext.

3. The IV is a part of the RC4 encryption key. The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a deadly analytic attack, that recovers the key, after intercepting and analyzing only a relatively small amount of traffic. This attack has been reduced to script.

4. WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a noncryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledges packets with the correct checksum. The combination of noncryptographic checksums with stream ciphers is dangerous and often leads to unintended “side channel” attacks, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP, and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now generally believed that it is risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text.

Note that only one of the four problems listed above depends on a weakness in the cryptographic algorithm. Therefore, the other three problems would not be improved by substituting a stronger stream cipher.

The third problem listed above is in part a consequence of a weakness in the RC4 stream cipher, but is only exposed by a poorly designed protocol.

Some of the problems associated with WEP and 802.11b WLAN security are summarized in Figure 7-11

Security Issue / Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a compromise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent brute-force attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

Figure 7.11. Key Problems with Existing 802.11 Wireless LAN Security

7.3.3.1 Monitoring

Despite the difficulty of decoding a 2.4GHz digital signal, hardware to listen to 802.11 transmissions is readily available to attackers in the form of consumer 802.11 products. The products possess all the necessary monitoring capabilities, and all that remains for attackers is to convince it to work for them.

Although most 802.11 equipment is designed to disregard encrypted content for which it does not have the key, we have been able to successfully intercept WEP-encrypted transmissions by changing the configuration of the drivers. We were able to confuse the firmware enough that the ciphertext (encrypted form) of unrecognized packets was returned to us for further examination and analysis.

Active attacks (those requiring transmission, not just monitoring) appear to be more difficult, yet not impossible. Many 802.11 products come with programmable firmware, which can be reverse-engineered and modified to provide the ability to inject traffic to attackers. Granted, such reverse-engineering is a significant time investment (we have not done this ourselves), but it's important to note that it's a one time cost. A competent group of people can invest this effort and then distribute the rogue firmware through underground circles, or sell it to parties interested in corporate espionage. The latter is a highly profitable business, so the time investment is easily recovered.

7.4 Security Requirements and Threats

As discussed above, the 802.11b WLAN industry is burgeoning and currently has significant momentum. All indications suggest that in the coming years numerous organizations will deploy 802.11b WLAN technology. Many organizations—including retail stores, hospitals, airports, and business enterprises—plan to capitalize on the benefits of “going wireless.” However, although there has been tremendous growth and success, everything relative to 802.11b WLANs has not been positive.

There have been numerous published reports and papers describing attacks on 802.11 wireless and exposing risks to any organization deploying the technology. This subsection will briefly cover the risks to security—i.e., attacks on confidentiality, integrity, and network availability.

Figure 7-12 provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against WLANs.

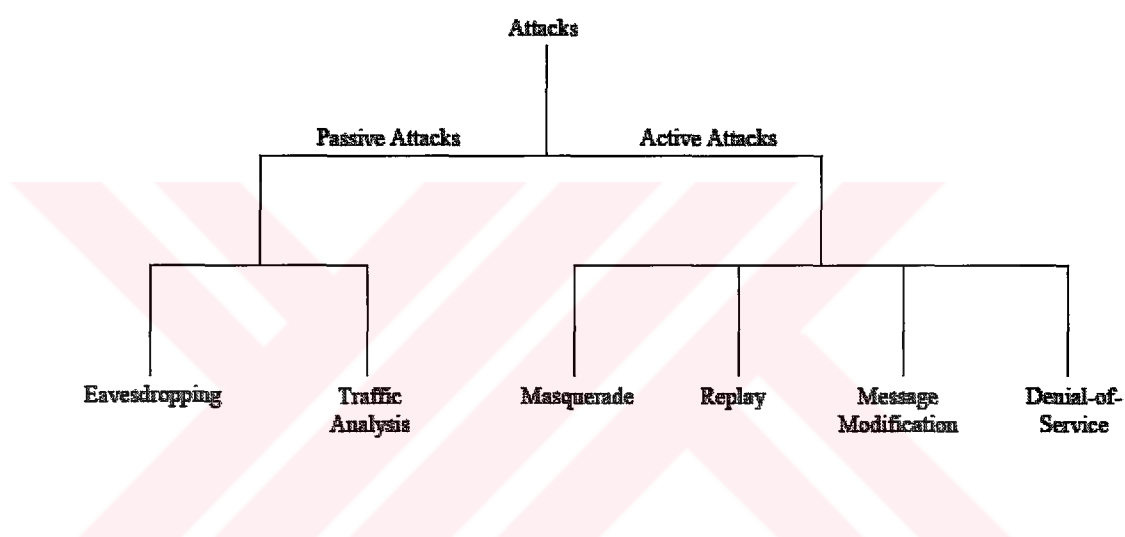


Figure 7.12. Taxonomy of Security Attacks

As Figure 7-12 shows, network security attacks are typically divided into *passive* and *active* attacks. These two broad classes are then subdivided into other types of attacks. All are defined below.

Passive Attack—An attack in which an unauthorized party simply gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either simple eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below. —

Eavesdropping—The attacker simply monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

—

Traffic analysis—The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

Active Attack—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.

Masquerading—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

Replay—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

Message modification—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

Denial-of-service—The attacker prevents or prohibits the normal use or management of communications facilities. All risks against 802.11 are the result of one or more of these attacks. The consequences of these attacks include loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service.

7.4.1 Loss of Confidentiality

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

This is, in general, a fundamental security requirement for most organizations. Due to the broadcast and radio nature of wireless, confidentiality is typically a more difficult security requirement to meet. Adversaries do not have to tap into a network cable to access network resources. Moreover, it may not be possible to control the distance over which the transmission occurs. This makes traditional physical security countermeasures less effective. Passive eavesdropping of native 802.11b wireless communications may cause significant risk to an organization. An adversary may be able to listen in and obtain sensitive information including proprietary information, network IDs and passwords, and configuration data. This risk is present because the 802.11b signals may travel outside the building perimeter or because there may be an “insider.” Because of the extended range of 802.11 broadcasts, adversaries can potentially detect transmission from a parking lot or nearby roads.

This kind of attack, performed through the use of a wireless network analyzer tool or *sniffer*, is particularly easy for two reasons: 1) frequently confidentiality features of WLAN technology are not even enabled, and 2) because of the numerous vulnerabilities in the 802.11b technology security, as discussed above, determined adversaries can compromise the system. Wireless packet analyzers, such as AirSnort and WEPcrack, are tools that are readily available on the Internet today. AirSnort is one of the first tools created to automate the process of analyzing networks. Unfortunately, it is also commonly used for breaking into wireless networks. AirSnort can take advantage of flaws in the key-scheduling algorithm of RC4, which forms part of the WEP standard. To accomplish this, AirSnort requires only a computer running the Linux operating system and a wireless network card. The software passively monitors the WLAN data transmissions and computes the encryption keys after at least 100MB of network packets have been *sniffed*. On a highly saturated network, collecting this amount of data may only take three or four hours; if traffic volume is low, a few days. After the network packets have been received, the fundamental keys may be guessed in less than one second. Once the malicious user knows the root key, that person can read any packet traveling over the WLAN.

Such sniffing tools' wide availability, ease of use, and ability to compute keys makes it essential for security administrators to implement secure wireless solutions.

Another risk to loss of confidentiality through simple eavesdropping is broadcast monitoring. An adversary can monitor traffic, using a laptop in promiscuous mode, when an access point is connected to a hub instead of a switch. Hubs generally broadcast all network traffic to all connected devices, which leaves the traffic vulnerable to unauthorized monitoring. For example, if a wireless access point was connected to an Ethernet hub, a device that is monitoring broadcast traffic could pick up data intended for wireless clients. Consequently, organizations should consider using switches instead of hubs for connections to wireless access points

WLANs risk loss of confidentiality following an active attack as well. Sniffing software as described above can obtain user names and passwords (as well as any other data traversing the network) as they are sent over a wireless connection. An adversary may be able to masquerade as a legitimate user and gain access to the wired network from an AP. Once "on the network," the intruder can scan the network using software available off the Internet.

The malicious eavesdropper then uses the user name, password, and IP address information to gain access to network resources and sensitive corporate data. Lastly, rogue APs pose a security risk. A malicious user could, physically and surreptitiously, insert a rogue AP into a closet, under a conference room table, or any other hidden area within a building and use it to gain access to the network. As long as its location is in close proximity to the users of the WLAN, the rogue AP can intercept the wireless traffic between an authorized AP and wireless clients. It need only be configured with a stronger signal than the existing AP to intercept the client traffic. A malicious user can also gain access to the wireless network through APs that are configured to allow access without authorization.

7.4.2 Loss of Integrity

Data integrity issues in wireless networks are similar to those in wired networks. Since organizations frequently implement wireless and wired communications without adequate cryptographic protection of data, integrity can be difficult to achieve. A hacker, for example, can compromise data integrity by deleting or modifying the data in an e-mail from an account on the wireless system. Depending on the importance of the e-mail and how widespread its distribution among e-mail recipients, the impact could be detrimental to an organization. Because the existing security features of 802.11 do not provide for strong message integrity, other kinds of active attacks are possible that compromise system integrity. As discussed before, the WEP-based integrity mechanism is simply a linear CRC. Message modification attacks are possible without the use of cryptographic checking mechanisms such as message authentication codes and hashes.

7.4.3 Loss of Network Availability

A denial in network availability involves some form of DoS attack, such as jamming. Jamming occurs when a malicious user deliberately emanates a signal from a wireless device in order to overwhelm legitimate wireless signals. Jamming results in a breakdown in communications since legitimate wireless signals are unable to communicate on the network.

Non-malicious users can also cause a DoS. A user, for instance, may unintentionally monopolize a wireless signal by downloading large files, effectively denying other users access to the network. As a result, organizational policies should limit the types and amounts of data that users are able to download on wireless networks.

7.4.4 Other Security Risks

With the prevalence of wireless devices, more users are seeking ways to connect remotely to their own organizations' networks. One such method is the use of untrusted, third party networks. Conference centers, for example, commonly provide wireless networks for users to connect to the Internet and subsequently to their own organizations while at the conference. Airports and even some coffee franchises are beginning to do the same. Starbucks and Boingo, for instance, are planning to deploy 802.11-based publicly accessible wireless networks for their customers, even offering virtual private network (VPN) capabilities for added security.

These untrusted public networks introduce three primary risks: 1) because they are public, they are accessible by anyone, even malicious users; 2) they serve as a bridge to a user's own network, thus potentially allowing anyone on the public network to attack or gain access to the bridged network; and 3) they use high RF transmission power levels for a strong signal strength, thus allowing malicious users to eavesdrop more readily on their signals.

In connecting to their own networks via an untrusted network, users may create vulnerabilities for their company networks and systems unless their organizations take steps to protect their users and themselves. Users typically need to access resources that their organizations deem as either public or private. Organizations should protect their public resources using an application layer security protocol such as Transport Layer Security (TLS), the Internet Engineering Task Force standardized version of Secure Sockets Layer (SSL). For private resources, organizations should use a VPN solution to secure their connections, since this will help prevent eavesdropping and unauthorized access to private resources. Lastly, as with any network, social engineering and dumpster diving are also concerns. An enterprise should consider all aspects of network security when planning to deploy the wireless network.

7.5 Risk Mitigation

Government organizations can mitigate risks to their WLANs by applying countermeasures to address specific threats and vulnerabilities. Management countermeasures combined with operational and technical countermeasures can be effective in reducing the risks associated with WLANs. The following guidelines will not prevent all adversary penetrations, nor will these countermeasures necessarily guarantee a secure wireless networking environment. This section describes risk-mitigating steps for an organization, recognizing that it is impossible to remove all risks. Additionally, it should be clear that there is no “one size fits all” when it comes to security. Some organizations may be able or willing to tolerate more risk than others. Also, security comes at a cost: either in dollars spent on security equipment, in inconvenience and maintenance, or in operating expenses. Some organizations may be willing to accept risk because applying various countermeasures may exceed financial or other constraints.

7.5.1 Management Countermeasures

Management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy, and compliance therewith, is the foundation on which other countermeasures—the operational and technical—are rationalized and implemented. A WLAN security policy should be able to do the following:

- Identify who may use WLAN technology in an organization
- Identify whether Internet access is required
- Describe who can install access points and other wireless equipment
- Provide limitations on the location of and physical security for access points
- Describe the type of information that may be sent over wireless links
- Describe conditions under which wireless devices are allowed

- Define standard security settings for access points
- Describe limitations on how the wireless device may be used, such as location
- Describe the hardware and software configuration of any access device
- Provide guidelines on reporting losses of wireless devices and security incidents
- Provide guidelines on the use of encryption and other security software
- Define the frequency and scope of security assessments

Another management countermeasure is to ensure that all critical personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the security risks that WLANs and devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack. Finally, the most important countermeasures are trained and aware users.

7.5.2 Operational Countermeasures

Physical security is the most fundamental step for ensuring that only authorized users have access to wireless computer equipment. Physical security combines such measures as access controls, personnel identification, and external boundary protection. As with facilities housing wired networks, facilities supporting wireless networks need physical access controls. For example, photo identification, card badge readers, or biometric devices can be used to minimize the risk of improper penetration of facilities. Some possible access mechanisms are proximity methods such as keypads or cipher locks. Biometric systems for physical access control include palm scans, hand geometry, iris scans, retina scans, fingerprint, voice pattern, signature dynamics, or facial recognition. External boundary protection can include locking doors and installing video cameras for surveillance around the perimeter of a site to discourage unauthorized access to wireless networking components such as wireless APs. It is important to consider the range of the AP when deciding where to place an AP in a WLAN environment. If the range extends beyond the physical boundaries of the office building walls, the extension creates a security vulnerability.

An individual outside of the building, perhaps “wardriving,” could eavesdrop on network communications by using a wireless device that picks up the RF emanations. A similar consideration applies to the implementation of building-to-building bridges. Ideally, the APs should be placed strategically within a building so that the range does not exceed the physical perimeter of the building and allow unauthorized personnel to eavesdrop near the perimeter.

Organizations should use site survey tools (see next paragraph) to measure the range of AP devices, both inside and outside of the building where the wireless network is located. In addition, organizations should use wireless security assessment tools (e.g., vulnerability assessment) and regularly conduct scheduled security audits.

Site survey tools are available to measure and secure AP coverage. The tools, which some vendors include with their products, measure the received signal strength from the APs. These measurements can be used to map out the coverage area. However, security administrators should use caution when interpreting the results since each vendor interprets the received signal strength differently. Some AP vendors also have special features that allow control of power levels and therefore the range of the AP. Such control is useful if the required coverage range is not broad because, for example, to the building or room in which access to the wireless network is needed happens to be small. Controlling the coverage range for this smaller building or room may help prevent the wireless signals from extending beyond the intended coverage area. Organizations could additionally use directional antennas to control emanations. However, directional antennas do not protect network links; they merely help control coverage range.

Although mapping the coverage area may yield some advantage relative to security, it should not be seen as an absolute solution. There is always the possibility that an individual might use a high-gain antenna to eavesdrop on the wireless network traffic. It should be recognized that only through the use of strong cryptographic means can a user gain any assurance against true eavesdropping adversaries.

The following paragraphs discuss how cryptography (Internet Protocol Security [IPsec] and VPNs) can be used to thwart many attacks.

7.5.3 Technical Countermeasures

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment. Software countermeasures include proper AP configurations (i.e., the operational and security settings on an AP), software patches and upgrades, authentication, intrusion detection systems (IDS), and encryption. Hardware solutions include smart cards, VPNs, public key infrastructure (PKI), and biometrics.

7.5.3.1 Software Solutions

Technical countermeasures involving software include properly configuring access points, regularly updating software, implementing authentication and IDS solutions, performing security audits, and adopting effective encryption. These are described in the paragraphs below

Access Point Configuration

Network administrators need to configure APs in accordance with established security policies and requirements. Properly configuring administrative passwords, encryption settings, reset function, automatic network connection function, Ethernet Medium Access Control (MAC) Access Control Lists (ACL), shared keys, and Simple Network Management Protocol (SNMP) agents will help eliminate many of the vulnerabilities inherent in a vendor's software default configuration.

Updating default passwords : Each WLAN device comes with its own default settings, some of which inherently contain security vulnerabilities. The administrator password is a prime example.

On some APs, the factory default configuration does not require a password (i.e., the password field is blank). Unauthorized users can easily gain access to the device if there is no password protection. Administrators should change default settings to reflect the organization's security policy, which should include the requirement for strong (i.e., an alphanumeric and special character string at least eight characters in length) administrative passwords. If the security requirement is sufficiently high, an organization should consider using an automated password generator. An alternative to password authentication is two-factor authentication. One form of two-factor authentication uses a symmetric key algorithm to generate a new code every minute. This code is a one-time use code that is paired with the user's personal identification number (PIN) for authentication. Another example of two-factor authentication is pairing the user's smart card with the user's PIN. This type of authentication requires a hardware device reader for the smart card or an authentication server for the PIN. Several commercial products provide this capability. However, use of an automated password generator or two-factor authentication mechanism may not be worth the investment, depending on the organization's security requirements, number of users, and budget constraints.

Establishing proper encryption settings : Encryption settings should be set for the strongest encryption available in the product, depending on the security requirements of the organization. Typically, APs have only a few encryption settings available: none, 40-bit shared key, and 128-bit shared key (with 128-bit being the strongest). Encryption as used in WEP, simple stream cipher generation, and exclusive-OR processing does not pose an additional burden on the computer processors performing the function. Consequently, organizations do not need to worry about computer processor power when planning to use encryption with the longer keys. However, it should be noted that some attacks against WEP yield deleterious results regardless of the key size.

Controlling the reset function : The reset function poses a particular problem because it allows an individual to negate any security settings administrators have

configured in the AP. It does this by returning the AP to its default factory settings. The default settings generally do not require an administrative password, for example, and may disable encryption. An individual can reset the configuration to the default settings simply by inserting a pointed object such as a pen into the reset hole and pressing. If a malicious user gains physical access to the device, that individual can exploit the reset feature and cancel out any security settings on the device. The reset function, if configured to erase basic operational information such as IP address or keys, can further result in a network DoS, because APs may not operate without these settings. Having physical access controls in place to prevent unauthorized users from resetting APs can mitigate the threats. Organizations can detect threats by performing regular security audits.

Using MAC ACL functionality : A MAC address is a hardware address that uniquely identifies each computer (or attached device) on a network. Networks use the MAC address to help regulate communications between different computer NICs on the same network subnet. Many 802.11 product vendors provide capabilities for restricting access to the WLAN based on MAC ACLs that are stored and distributed across many APs. The MAC ACL grants or denies access to a computer using a list of permissions designated by MAC address.

However, the Ethernet MAC ACL does not represent a strong defense mechanism by itself. Because MAC addresses are transmitted in the clear from a wireless NIC to an AP, the MAC can be easily captured. Malicious users can spoof a MAC address by changing the actual MAC address on their computer to a MAC address that has access to the wireless network. This countermeasure may provide some level of security; however, users should use this with caution. This may be effective against casual eavesdropping but will not be effective against determined adversaries. Users may want to consider this as part of an overall defense-in-depth strategy—adding levels of security to reduce the likelihood of problems.

However, users should weigh the administrative burden of enabling the MAC ACL (assuming they are using MAC ACLs) against the true security provided. In a medium to large network, the burden of establishing and maintaining MAC ACLs may exceed the value of the security countermeasure.

Changing the SSID : The SSID of the AP must be changed from the factory default. Although an equipped adversary can capture this identity parameter over the wireless interface, it should be changed to prevent unsophisticated adversary attempts to connect to the wireless network.

Changing default cryptographic keys : The manufacturer may provide one or more keys to enable shared key authentication between the device trying to gain access to the network and the AP. Using a default shared key setting is a security vulnerability because many vendors use identical shared keys in their factory settings. A malicious user may know the default shared key and use it to gain access to the network. Changing the default shared key setting to another key will mitigate the risk. For example, the shared key could be changed to “954617” instead of using a factory default shared key of “111111.” No matter what their security level, organizations should change the shared key from the default setting because it is easily exploited. In general, organizations should opt for strong encryption (e.g., 128-bit), regardless of their security levels, whenever it is available. If it is not available or feasible, organizations should, assuming they have already performed a risk analysis, use 40-bit encryption. Finally, a generally accepted principle for proper key management is to change cryptographic keys often.

Changing default SNMP Parameter : Some wireless APs use *SNMP* agents, which allow network management software tools to monitor the status of wireless APs and clients. The default SNMP community string that SNMP agents commonly use is the word “public” with assigned “read” or “read and write” privileges. Using this well-known default string leaves devices vulnerable to attack. If an unauthorized user were to gain access and had read/write privileges, that user could write data to the AP, resulting

in a data integrity breach. Organizations that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to “read only” if that is the only access a user requires. If SNMP is not required on the network, the organization should disable SNMP altogether.

Changing default channel. :One other consideration that is not directly exploitable is the default channel. Vendors commonly use default channels in their APs. If two or more APs are located near each other but are on different networks, a DoS can result from radio interference between the two APs. Organizations that incur radio interference need to determine if a nearby AP(s) is using the same channel or a channel within five channels of their own, and then choose a channel that is in a different range.

Using DHCP : Automatic network connections involve the use of a Dynamic Host Control Protocol (DHCP) server. The DHCP server automatically assigns IP addresses to devices that associate with an AP when traversing a subnet. For example, a DHCP server is used to manage a range of TCP/IP addresses for client laptops or workstations. After the range of IP addresses is established, the DHCP server dynamically assigns addresses to workstations as needed. The server assigns the device a dynamic IP address as long as the encryption settings are compatible with the WLAN. The threat with DHCP is that a malicious user could easily gain unauthorized access on the network through the use of a laptop with a wireless NIC. Since a DHCP server will not necessarily know which wireless devices have access, the server will automatically assign the laptop a valid IP address. Risk mitigation involves disabling DHCP and using static IP addresses on the wireless network, if feasible. This alternative, like the MAC ACL countermeasure, may only be practical for relatively small networks, given the administrative overhead involved with assigning static IP addresses and the possible shortage of addresses. Statically assigning IP addresses would also negate some of the key advantages of wireless networks, such as roaming or establishing ad hoc networks.

Another possible solution is to implement a DHCP server inside of the wired network's firewall that grants access to a wireless network located outside of the wired network's firewall. Still another solution is to use APs with integrated firewalls. This last solution will add an additional layer of protection to the entire network. All users should evaluate the need for DHCP taking into consideration the size of their network.

Software Patches and Upgrades

Vendors generally try to correct known software (and hardware) security vulnerabilities when they have been identified. These corrections come in the form of security patches and upgrades. Network administrators need to regularly check with the vendor to see whether security patches and upgrades are available and apply them as needed.

An example of a software or firmware patch is the one related to the RSA Security WEP security enhancement. In November 2001, RSA Security, Inc., developed a technique for the security holes found in WEP. This enhancement, referred to as "fast packet keying," generates a unique key to encrypt each network packet on the WLAN. The IEEE has approved the fast packet keying technology as one fix to the 802.11 protocol. Vendors have started applying the fix to new wireless products and have developed software patches for many existing products. Organizations should check with their individual vendors to see if patches are available for the products they have already purchased.

Authentication :In general, effective authentication solutions are a reliable way of permitting only authorized users to access a network. Authentication solutions include the use of usernames and passwords; smart cards, biometrics, PKI; or a combination of solutions (e.g., smart cards with PKI). When relying on usernames and passwords for authentication, it is important to have policies specifying minimum password length, required password characters, and password expiration.

Smart cards, biometrics, and PKI have their own individual requirements and will be addressed in greater detail later in the document. All organizations should implement a strong password policy, regardless of the security level.

Strong passwords are simply a fundamental measure in any environment. Organizations further should consider other types of authentication mechanisms (e.g., smart cards with PKI) if their security levels warrant additional authentication. These mechanisms may be integrated into a WLAN solution to enhance the security of the system. However, users should be careful to fully understand the security provided by enhanced authentication. This does not in and of itself solve all problems. For example, a strong password scheme used for accessing parameters on a NIC card does nothing to address the problems with WEP cryptography.

Personal Firewalls : Resources on public wireless networks have a higher risk of attack since they generally do not have the same degree of protection as internal resources. Personal firewalls offer some protection against certain attacks. Personal firewalls are software-based solutions that reside on a client's machine and are either client-managed or centrally managed. Client-managed versions are best suited to low-end users because individual users are able to configure the firewall themselves and may not follow any specific security guidelines. Centrally managed solutions provide a greater degree of protection because IT departments configure and remotely manage them.³⁵ Centrally managed solutions allow organizations to modify client firewalls to protect against known vulnerabilities and to maintain a consistent security policy for all remote users. Some of these high-end products also have VPN and audit capabilities. Although personal firewalls offer some measure of protection, they do not protect against advanced forms of attack. Depending on the security requirement, organizations may still need additional layers of protection.

Intrusion Detection System : An IDS is an effective tool for determining whether unauthorized users are attempting to access, have already accessed, or have

compromised the network. IDS for WLANs can either be host-based or network-based. A host-based IDS adds a targeted layer of security to particularly vulnerable or essential systems. A host-based agent is installed on an individual system (for example, a database server) and monitors audit trails and system logs for suspicious behavior, such as repeated failed login attempts or changes to file permissions. The agent may also employ a checksum at regular intervals to look for changes to system files. In some cases, an agent can halt an attack on a system, although a host agent's primary function is to log and analyze events and send alerts.

A network-based IDS monitors the LAN (or a LAN segment) network traffic, packet by packet, in real time (or as near to real time as possible) to determine whether traffic conforms to predetermined attack signatures (activities that match known attack patterns). For example, the TearDrop DoS attack sends packets that are fragmented in such a way as to crash the target system. The network monitor will recognize packets that conform to this pattern and take action such as killing the network session, sending an e-mail alert to the administrator, or other action specified. Host-based systems have an advantage over network-based IDS when encrypted connections, e.g., SSL web sessions or on VPN connections, are involved. Because the agent resides on the component itself, the host-based system is able to examine the data after it has been decrypted. In contrast, a network-based IDS is not able to decrypt data; therefore, encrypted network traffic is passed through without investigation. (For more information about IDS, see NIST Special Publication 800-21, *Intrusion Detection Systems*.) Users requiring high levels of security should implement an IDS because it provides an added layer of security. Low-end users should consider an IDS as well but only if it is financially feasible. In addition to the cost of the system itself, an IDS requires staff to monitor and react to IDS events and to provide general administration to the IDS database and components.

Encryption : As mentioned earlier, APs generally have only three encryption settings available: none, 40-bit shared key, and 104-bit. “None” represents the most serious risk

since unencrypted data traversing the network can easily be intercepted, read, and altered. A 40-bit shared key will encrypt the network communications data, but there is still a risk of compromise. The 40-bit encryption has been broken by brute force cryptanalysis using a high-end graphics computer and even low-end computers; consequently, it is of questionable value. In general, 104-bit encryption is more secure than 40-bit encryption because of the significant difference in the size of the cryptographic keyspace. Although this is not true for 802.11 WEP because of poor cryptographic design using IVs as discussed previously, it is recommended nonetheless as a “good practice.” Again, users of 802.11b APs and wireless client should be vigilant about checking with the vendor regarding upgrades to firmware and software as they may overcome some of the WEP problems.

Security Assessments : Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it remains secure. It is important for organizations to perform regular audits using wireless network analyzers and other tools. An analyzer, again, sometimes called a sniffer, is an effective tool to conduct security auditing and troubleshoot wireless network issues. Security administrators or security auditors can use network analyzers, such as Netstumbler (see <http://www.netstumbler.com/>), to determine if wireless products are transmitting correctly and on the correct channels.

Administrators should periodically check within the office building space (and campus) for rogue APs and against other unauthorized access. Organizations may also consider using an independent third party to conduct the security audits. Such organizations are, generally, many times more up-to-date on security vulnerabilities, better trained on security solutions, and equipped to assess the security of a wireless network. An independent third-party audit, which may include penetration testing, will help an organization ensure that its WLAN is compliant with established security procedures and policies, and that the system is up-to-date with the latest software patches and upgrades.

It is worth noting that organizations should take a holistic approach to the assessment process. It is important to ensure that the wireless portion of the network is secure but it is also important for the wired portion to be secure as well.

7.5.3.2 Hardware Solutions

Hardware countermeasures for mitigating WLAN risks include implementing smart cards, VPNs, PKI, biometrics, and other hardware solutions.

Smart Cards

Smart cards may add another level of protection, although they also add another layer of complexity. Organizations can use smart cards in conjunction with username or password or by themselves. They can use smart cards in two-factor authentication (see above). Organizations can also combine smart cards with biometrics.

In wireless networks, smart cards provide the added feature of authentication. Smart cards are beneficial in environments requiring authentication beyond simple username and password. User certificate and other information are stored on the cards themselves and generally require the user only to remember a PIN number. Smart cards are also portable; consequently users can securely access their networks from various locations. As with an authentication software solution, these tamper-resistant devices may be integrated into a WLAN solution to enhance the security of the system. Again, users should be careful to fully understand the security provided by the smart card solution. These alone will not solve all the problems of 802.11 security.

Virtual Private Networks

VPN technology is a rapidly growing technology to provide secure data transmission across public network infrastructures. VPNs have in recent years allowed corporations to harness the power of the Internet for remote access. Today, VPNs are typically used in three different scenarios: for remote user access, for LAN-to-LAN (site-to-site) connectivity, and for extranets.

VPNs employ cryptographic techniques to protect IP information as it passes from one network to the next or from one location to the next. Data that is inside the VPN “tunnel”—the encapsulation of one protocol packet inside another—is encrypted and isolated from other network traffic. A VPN for site-to-site connectivity is illustrated in Figure 7-13. In this scenario, traffic communicated from Site A to Site B is protected as it moves across the Internet. Confidentiality, integrity, and other security services are provided as discussed below.

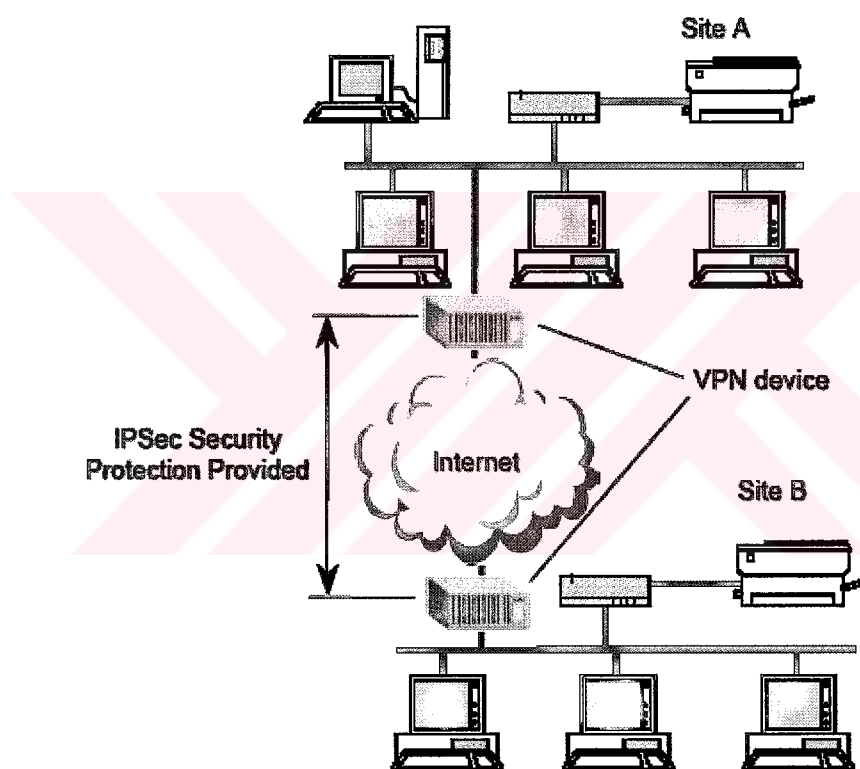


Figure 7.13. Typical Use of VPN for Secure Internet Communications from Site-to-Site

Most VPNs in use today make use of the IPsec protocol suite. IPsec, developed by the Internet Engineering Task Force (IETF), is a framework of open standards for ensuring private communications over IP networks. It provides the following types of robust protection:

- Confidentiality
- Connectionless integrity
- Data origin authentication
- Replay protection
- Traffic analysis protection.

Connectionless integrity guarantees that a received message has not changed from the original message. Data origin authentication guarantees that the received message was sent by the originator and not by a person masquerading as the originator. Replay protection provides assurance that the same message is not delivered multiple times, and that messages are not out of order when delivered.

Confidentiality ensures that others cannot read the information in the message. Traffic analysis protection provides assurance that an eavesdropper cannot determine who is communicating or the frequency or volume of communications. IPsec accomplishes the task of routing the messages via an encrypted tunnel by two special IPsec headers inserted immediately after the IP header in each message. The Encapsulating Security Protocol (ESP) header provides privacy and protects against malicious modification, and the Authentication header (AH) protects against modification without providing privacy. The Internet Key Exchange (IKE) Protocol is a mechanism that allows for secret keys and other protection-related parameters to be exchanged prior to a communication without the intervention of a user.

The use of IPsec with WLANs is depicted in Figure 7-13. As shown, the IPsec tunnel is provided from the wireless client through the AP to the VPN device on the enterprise network edge.

With IPsec, security services are provided at the network layer of the protocol stack. This means all applications and protocols operating above that layer (i.e., above layer 3) are IPsec protected. The IPsec security services are independent of the security that is occurring at layer 2, the WEP security. As a defense-in-depth strategy, if a VPN is in place, an organization can consider having both IPsec and WEP applied. With a configuration as in Figure 7-14, the VPN encrypts (and otherwise protects) the transmitted data to and from the wired network.

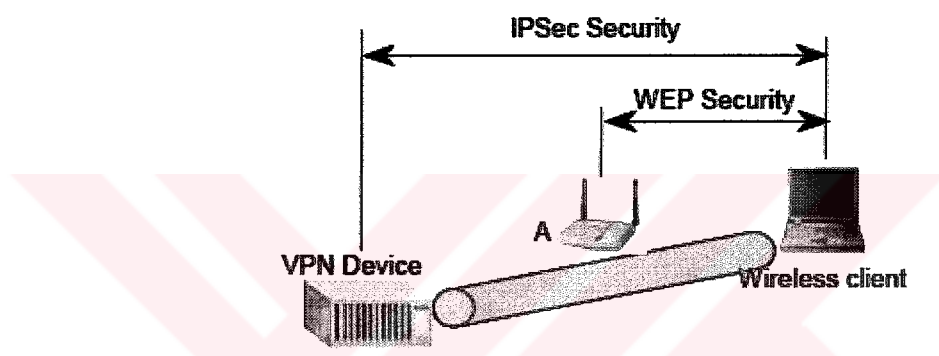


Figure 7.14. VPN Security In addition to WEP

Figure 7-15 illustrates another example of a wireless network with the “VPN overlay.” As shown, with wireless devices with VPNs, clients can connect securely to the enterprise network through a VPN gateway on the enterprise edge.

Wireless clients establish IPsec connections to the wireless VPN gateway—in addition to or in substitute for WEP. Note that the wireless client does not need special hardware; it just needs to be provided with IPsec/VPN client software. The VPN gateway can use preshared cryptographic keys or digital certificates (public-key based) for wireless client device authentication. Additionally, user authentication to the VPN gateway can occur using Remote Authentication Dial-In User Service (RADIUS) or one-time-passwords (OTP) generated with SecureID, for example. The VPN gateway may or may not have an integral firewall to restrict traffic to certain locations within the enterprise network.

Additionally, the VPN gateway may or may not have the ability to create an audit journal of all activities. An audit trail is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities. A security manager may be able to use an audit trail on the VPN gateway to monitor compliance with security policy and to gain an understanding of whether only authorized persons have gained access to the wireless network.

It should be noted that although the VPN approach enhances the air-interface security significantly, this approach does not completely address security on the enterprise network. For example, authentication and authorization to a particular enterprise application are not addressed with this security solution. Organizations may want to seek assistance in developing a comprehensive enterprise security strategy.

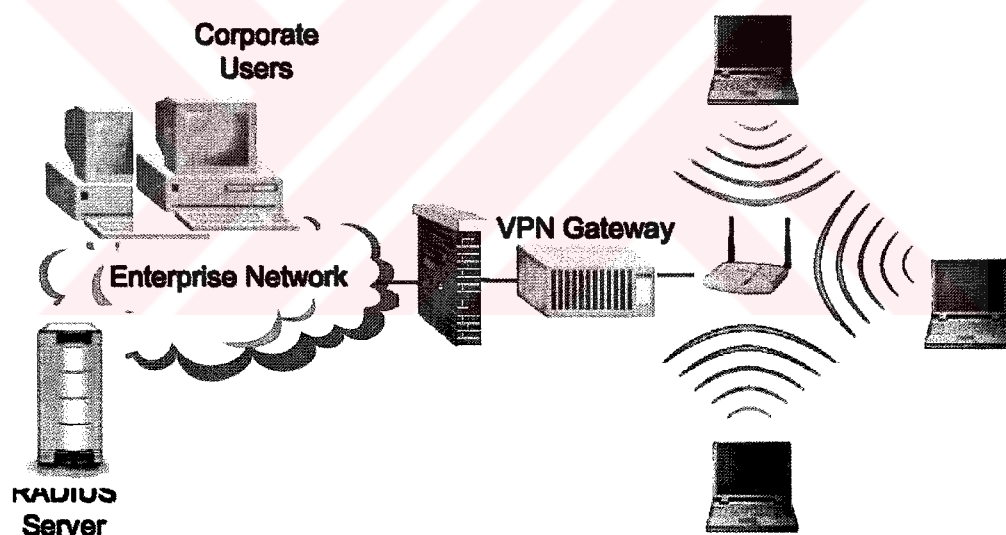


Figure 7.15. Simplified Diagram of VPN WLAN

Public Key Infrastructure

PKI provides the framework and services for the generation, production, distribution, control, and accounting of public key certificates.

It provides applications with secure encryption and authentication of network transactions as well as data integrity and non-repudiation, using public key certificates to do so. WLANs can integrate PKI for authentication and secure network transactions. Third-party manufacturers, for instance, provide wireless PKI, handsets, and smart cards that integrate with WLANs.

Users requiring high levels of security should strongly consider PKI. It provides strong authentication through user certificates and users can use those same certificates with application-level security, such as signing and encrypting (i.e., using encryption certificates) messages. Smart cards provide even greater utility (e.g., portability, mobility) since the certificates are integrated in the card. Users requiring lower levels of security, on the other hand, need to consider carefully the complexity and cost of implementing and administering a PKI before adopting this solution.

Biometrics

Biometric devices include fingerprint/palm-print scanners, optical scanners (including retina and iris scanners), facial recognition scanners, and voice recognition scanners. Biometrics provides an added layer of protection when used either alone or along with another security solution.

For example, for organizations needing higher levels of security, biometrics can be integrated with wireless smart cards or wireless laptops or other wireless devices and used in lieu of username and password to access the wireless network. Additionally, biometrics can combine with VPN solutions to provide authentication and data confidentiality.

7.5.3.3 Other Hardware Solutions

The security industry has responded to the reports of vulnerabilities in WEP and 802.11b WLAN security.

Numerous products are currently available to address the vulnerabilities. Several vendors offer combined security solutions in a single product. Two such vendors, described here as examples, are Bluesocket and Vernier Networks. Bluesocket's Wireless Gateway 1000 (WG-1000) effectively creates a firewall between the wireless APs and the rest of the corporate network. The WG-1000 requires authentication via an internal database or a central corporate server. For centralized authentication, the WG-1000 supports RADIUS, Lightweight Directory Access Protocol (LDAP), NT 4 Domain and Windows 2000 Active Directory. In addition, Extensible Authentication Protocol (EAP) for token-based authentication is also supported. The use of roles is available to support assigning different encryption to different users depending on the level of security needed. Role assignment also supports a maximum bandwidth for each user category such as "employees" and "visitors." WG-1000 also supports strong encryption to overcome the weaknesses in WEP that are described in the encryption section above.

Vernier Networks has created the Vernier Networks System that consists of two hardware devices that authenticate, control, redirect, and log network traffic generated by each user's wireless network, cell phone, or other device without installing client software. The devices are the CS 5000 Control Server and the AM 5004 Access Manager.

The Control Server centrally manages authentication for all wireless users, coordinates layer 3 roaming, and enforces policies. The Access Manager resides at the edge of the network and connects to APs, enforces user rights for authenticated users, and enables roaming and other security functions such as IPsec, Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP).

These two products illustrate the numerous products that are available to secure the WLAN environment. Organizations that decide to investigate any potential solution should carefully consider the security features offered by various products and make sure that the residual risk, after the countermeasures are applied, is acceptable.

The other solution is using smartgate

Securing wireless communications with smartgate

Wireless Traffic without SmartGate

Wireless access points are connected to the enterprise network. Clients are equipped with either wireless NICs or built in capability. Wireless clients transmit data packets across radio frequencies determined by the type of 802.11 transmission specification they are using: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), or Infrared.

The wireless device, be it a handheld or laptop, will associate to an access point. If the 'key' or identity of the unit is confirmed, it will allow data packets to be transferred to the access point acting as a gateway to other wired services. These data packets may be encrypted by that same shared, but not unique, key. Once the data is received over the airwaves at the access point, it is delivered over wired networks directly to a local trusted network, intranet, or public Internet.

Because the wireless access points are directly connected to the enterprise network, unauthorized users can exploit weaknesses in WEP. This allows the rogue user access to the entire enterprise network.

"AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. AirSnort requires approximately 100M-1 GB of data to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. "

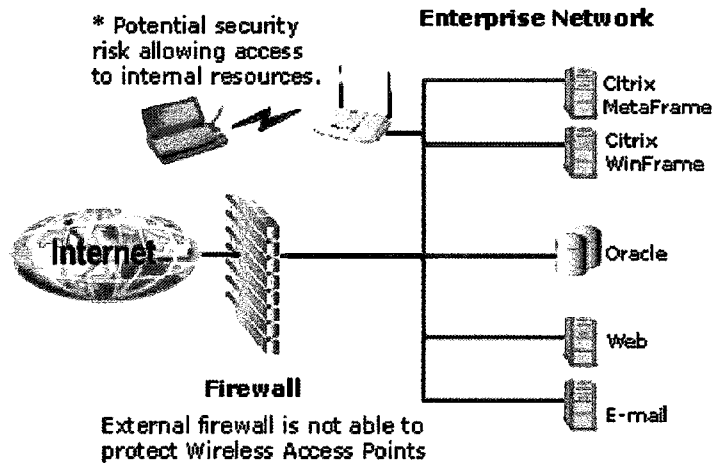


Figure 7.16 – Unsecured Wireless Access

Wireless communications with smartgate

V-ONE has products with firewall capabilities that can stop all unauthorized access to the enterprise network. Because V-ONE technology uses strong mutual authentication and changing session keys, tools like AirSnort are not able to gain access to the internal network. The wireless LAN is treated similar to the insecure public Internet.

Using V-ONE's products over wireless LANs provides true central configuration. If a wireless device is stolen, the administrator simply disables the account on the SmartGate server.

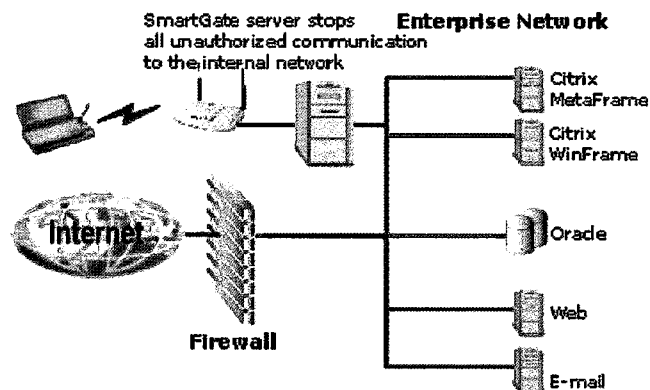


Figure 7.17 - Typical SmartGate Secured Architecture

V-ONE's VPN provides true security for wireless LANs:

- 9 Built-in firewall capability
- 9 3DES encryption – ensures secure transmission of data
- 9 Mutual authentication – ensures the identity of the person
- 9 Fine grain access control – ensures that the user accesses only “permitted data”
- 9 Easy and simple client management – easily manage updates and access privileges
- 9 Easy to use
- 9 On-line Registration (OLR) for rapid deployment
- 9 Simple client operation

7.6 Emerging Security Standards and Technologies

Like the security industry, standards organizations too have responded to the flurry over insecurities in 802.11b WLANs. Activity is occurring in the Internet Engineering Task Force (IETF) as well as the IEEE. The IEEE is currently working on three separate initiatives for improving WLAN security. The first involves the IEEE 802.11 Task Group i (TGi) which has proposed significant modifications to the existing IEEE 802.11 standard as a long-term solution for security. The TGi is defining a second version of WEP—based on the newly-released Advanced Encryption Standard (AES).

The AES-based solution will provide a highly-robust solution for the future but will require new hardware and protocol changes. TGi currently has design requirements to address all the known problems with WEP including the prevention of forgeries and detection of replay attacks.

The second initiative for improving WLAN security is the TGi's short-term solution to address the problems of WEP.

The group is defining the Temporal Key Integrity Protocol (TKIP) to address the problems without requiring hardware changes – that is, changes to firmware and software drivers only will be required. Again the primary goal of TKIP is, in the near-term, to remove all known vulnerabilities and allow operation on existing wireless-fidelity (Wi-Fi)-certified hardware. Wi-Fi certification is awarded by WECA, and this certification ensures that 802.11 devices with the certification are interoperable with other Wi-Fi certified 802.11 devices. The group seeks to produce the solution before the IEEE 802.11i standard is complete.

The third initiative from IEEE is the introduction of a new standard, IEEE 802.1x. The IEEE 802.1x standard defines a generic framework for port-based access control and key distribution. By using the existing Extensible Authentication Protocol (EAP), an AP authenticates a NIC by consulting an authentication server. The 802.1x standard supports authentication servers such as RADIUS or Kerberos. RADIUS is an authentication and accounting server for terminal servers that communicate in the RADIUS protocol. The 802.1x standard can be implemented with different EAP types, including EAP-MD5 for Ethernet LANs and EAP-Transport-level Security (TLS) for 802.11b WLANs. Currently numerous EAP-based protocols are being developed within the IETF, to work with 802.1x, in addressing the WEP WLAN problems

The 802.1x standard also addresses another serious omission in the WEP standard by providing for secure delivery of session keys. For example, session keys might be created as needed by the AP or supplied by a RADIUS server. If a malicious user recovered keys from WEP session traffic, the keys would be of no value for other sessions. This is an improvement from the original session key delivery method, which allowed session keys to be intercepted. If secure delivery of session keys was not in place, an attack could occur by intercepting the session keys.

It is the intent of the IEEE that with the introduction of 802.1x, in concert with EAP techniques from the IETF, some of the security vulnerabilities that have been exposed in the 802.11b standard can be eliminated.

7.7 A Simple Design: Implementing a Wireless LAN in the Work Environment

Organization A is considering implementing a WLAN so that employees may use their laptop computers anywhere within the boundaries of their office building. The security department first identifies WLAN vulnerabilities and threats. The department, assuming that threat-sources will try to exploit WLAN vulnerabilities, determines the overall risk of operating a WLAN and the impact a successful attack would have on Organization A. The manager reads the risk assessment and decides that the residual risk exceeds the benefit the WLAN provides. The manager directs the computer security department to identify additional countermeasures to mitigate residual risk before the system can be implemented.

Using the risk assessment as its basis, the computer security department concentrates on four areas for risk mitigation: physical security, AP location, AP configuration, and security policy. Analysis of physical security reveals that nonemployees are able to gain access to the building after checking in at the main desk. To ensure that only authorized employees and guests may access the building, the security department recommends that Organization A adopt the use of photo identification, card badges, or biometric devices. The security team will physically secure the APs by installing them within the secured building facility, which requires users to have proper identification to enter.

The computer security department wants to minimize the possibility that unauthorized users will access the WLAN from outside the building. The security department evaluates each AP to determine the network vulnerabilities such as eavesdropping. Network engineers conduct a site survey to determine the best physical location for the APs, to reduce the threat of eavesdropping. This involves physically mapping where users have wireless access to the network. The security department realizes that with a high-gain antenna, attackers will still be able to eavesdrop on wireless network traffic.

To offset this risk the department proposes placing the WLAN outside the firewall and passing traffic through a VPN that supports high-level encryption. This configuration will greatly reduce the risks associated with eavesdropping.

Next, the computer security department focuses on vulnerabilities related to AP configuration. Because many APs retain the original default factory password setting, the computer security department chooses a robust password to ensure a higher level of assurance. In conjunction with management and network administrators, the security department develops a security policy that requires passwords to be regularly updated and have a minimum length of eight alphanumeric characters. The policy includes the provision to change the encryption setting from “no encryption” to 128-bit encryption. The policy further deals with MAC ACL usage. To provide an additional level of access security, the department allows the use of MAC ACLs whenever possible. The policy also addresses the use of SNMP. The computer security department decides to disable remote SNMP because of the related threat and only allows it from internal hosts. Finally, since many vendors use default shared authentication keys, unauthorized devices can gain access to the network if they know the default key. Consequently, the security department stipulates the use of username and password as supplemental authentication to APs.

The security department adds additional policies to address software upgrades and use of the network. The policy requires system administrators to test and update security patches and upgrades, as soon as the vendor makes them available. Frequent patches and upgrades will help reduce the possibility of attack on the older, faulty version of the software.. The policy also strongly discourages users from processing proprietary or employee personal data when connected from their laptops to the WLAN, thus helping to reduce the risk of personnel data exploitation. Additionally, the policy states that if a laptop is lost or stolen, the employee to whom the laptop belongs will promptly notify the security department.

This will ensure that the security department can quickly identify the IP address assigned to the laptop and prevent that IP address from accessing the network.

As an additional security measure, the security department recommends that Organization A incorporate the use of an IDS.

The IDS will help determine whether unauthorized users are attempting to access, have already accessed, or have compromised the network. The department views an IDS as a useful tool in protecting Organization A's network and, more importantly, the data that traverses it.

The security department presents the manager with the risk assessment, which includes the countermeasures described above (and listed below) and a diagram (Figure 7-18) of the proposed WLAN. The risk assessment also includes an update of the residual risk with the proposed measures in place. Realizing that the benefits of system operation now outweigh the residual risks, the manager agrees to implement the WLAN. However, the security department warns that although the risk assessment is thorough, WLAN technology is continually changing along with the security vulnerabilities that malicious users expose. They offer encryption algorithms as an example. As encryption-breaking programs become more sophisticated, malicious users may expose more software flaws in vendor programs or weaknesses in encryption algorithms. They also point out that users always represent the weakest link in a security chain. The organization must continue to educate the user community about the risks that wireless technologies pose, reiterating, for example, how important it is not to give others their usernames and passwords and not to execute programs that come from unknown sources. In conclusion, the security department conveys that the strategy is one of defense-in-depth. They cite, for example, that WEP encryption will be enabled with random keys, MAC ACLs will be used, and a IPsec-based VPN overlay will be deployed. They also note that they will monitor the appropriate standards organizations and the availability of products such that the optimal security solution—most secure and cost-effective—for the enterprise can be determined.

Organization A's Proposed Countermeasures are as follows:

- ☐ ☐ Adopt personal identification system for physical access control
- ☐ ☐ Secure AP configuration
 - Choose robust password to ensure a higher level of security
 - Use 128-bit encryption
 - Create MAC ACLs and enable checking in APs
 - Change SSID from default setting and suppress its broadcast
 - Change WEP keys from default settings
 - Disable remote SNMP
- ☐ ☐ Conduct site survey and strategically place wireless APs
- ☐ ☐ Deploy VPN overlay (gateway and client) with integral firewall
- ☐ ☐ Establish comprehensive security policies regarding use of wireless devices
- ☐ ☐ Deploy personal firewalls and antivirus software on the wireless clients
- ☐ ☐ Investigate 802.11b products with best long-term wireless security strategy and longevity in marketplace
- ☐ ☐ Seek third-party assistance in conducting a security assessment after deployment

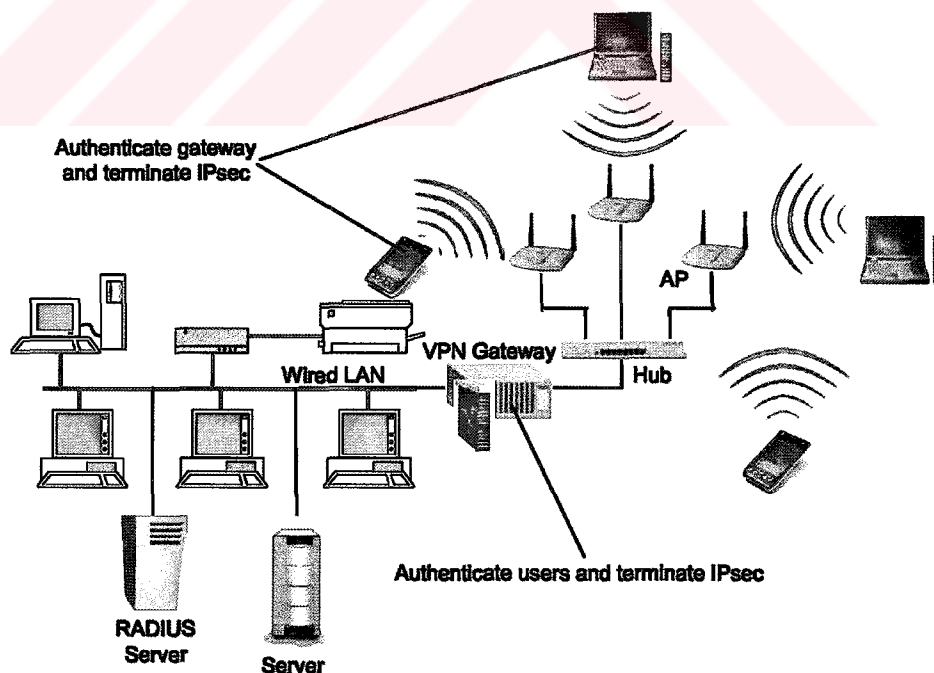


Figure 7.18. Organization A WLAN Architecture

7.8 Wireless LAN Security Checklist

Figure 7-19 provides a WLAN security checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network.

For each recommendation or guideline, three columns are provided. The first column, the *Best Practice* column, if checked, means this is something recommended of all organizations. The second column, the *May Consider* column, if checked, means the recommendation is something that an organization may want to carefully consider for three reasons. First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some sort of additional protection. Second, the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational or cost impacts. In summary, if the *May Consider* column is checked, organizations need to carefully consider the option and weigh the costs versus the benefits. The last column, the *Done?* column, is intentionally left blank and allows an organization to use this table as a true checklist. For instance, an individual performing a wireless security audit in an 802.11 environment can quickly check off each recommendation for the organization – asking, “Have I done this?”

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Develop an organizational security policy that addresses the use of wireless technology, including 802.11.	✓		
Ensure users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	✓		
Perform a risk assessment to understand the value of the assets in the organization that need protection.	✓		
Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they come available (prior to purchase).	✓		
Perform comprehensive security assessments at regular intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	✓		
Ensure external boundary protection is in place around the perimeter of the building or buildings of the organization.	✓		
Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
Complete a site survey to measure and establish the AP coverage for the organization.	✓		
Take a complete inventory of all APs and 802.11 wireless devices.	✓		
Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	✓		
Ensure AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	✓		
Locate APs on the interior of buildings versus near exterior walls and windows.	✓		
Place APs in secured areas to prevent unauthorized physical access and user manipulation.	✓		
Make sure that APs are turned off during all hours during they are not used.	✓		
Make sure the reset function on APs is being used only when needed and is only invoked by an authorized group of people.	✓		
Restore the APs to the latest security settings when the reset functions are used.	✓		
Change the default SSID in the APs.	✓		
Disable the "broadcast SSID" feature so that the client SSID must match that of the AP.	✓		
Validate that the SSID character string does not reflect the organization's name (division, department, street, etc.) or products.	✓		
Disable the broadcast beacon of the APs.		✓	
Understand and make sure all default parameters are changed.	✓		
Disable all insecure and nonessential management protocols on the APs.	✓		
Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.	✓		
Ensure that encryption key sizes are at least 128-bits or as large as possible.	✓		
Make sure that default shared keys are periodically replaced by more secure unique keys.	✓		
Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	✓		

Security Recommendation	Checklist		
	Best Practice	May Consider	Done
Install antivirus software on all wireless clients.		✓	
Install personal firewall software on all wireless clients.		✓	
Deploy MAC access control lists.		✓	
Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.		✓	
Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.		✓	
Ensure encryption being used is as strong as possible given the sensitivity of the data on the network and the processor speeds of the computers.		✓	
Fully test and deploy software patches and upgrades on a regular basis.	✓		
Ensure all APs have strong administrative passwords.	✓		
Ensure all passwords are being changed regularly.	✓		
Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.		✓	
Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable.	✓		
Use static IP addressing on the network.		✓	
Disable DHCP.		✓	
Enable user authentication mechanisms for the management interfaces of the AP.	✓		
Ensure management traffic destined for APs is on a dedicated wired subnet.		✓	
Make sure adequately robust community strings are used for SNMP management traffic on the APs.	✓		
Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used.	✓		
Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.		✓	
Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.		✓	
Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.		✓	
Deploy intrusion detection sensors on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		✓	
Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.		✓	
Wait until future releases of 802.11 WLAN technology that incorporates fixes to the security features or enhanced security features.		✓	

Figure 7.19. Wireless LAN Security Checklist

CHAPTER EIGHT

AD-HOC NETWORK

8. Ad Hoc Networks

This section provides a detailed overview of ad hoc networks, in particular, those based on Bluetooth technology. As mentioned earlier, ad hoc networks are a relatively new paradigm of wireless communications in which there is no fixed infrastructure such as base stations or access points. In ad hoc networks, devices maintain random network configurations formed “on-the-fly,” relying on a system of mobile routers connected by wireless links to enable devices to communicate with each other. Devices within an ad hoc network control the network configuration and maintain and share resources. Ad hoc networks are similar to P2P networking in that they both use decentralized networking, in which the information is maintained at the end user location rather than in a centralized database. However, ad hoc and P2P networks differ in that P2P relies on a routing mechanism to direct information queries, whereas ad hoc networks rely on the device hardware to request and share the information.

Ad hoc networks allow devices to access wireless applications, such as address book synchronization and file sharing, within a personal area network (PAN). When combined with other technologies, these networks can be expanded to include network and Internet access. Bluetooth devices that typically do not have access to network resources, but that are connected in a Bluetooth network with an 802.11 capable device, can achieve connection within the corporate network as well as reach out to the Internet.

8.1 Bluetooth Overview

Ad hoc networks today are based primarily on Bluetooth technology. Bluetooth is an open standard for short-range digital radio. It is touted as a low-cost, low-power, and low-profile technology that provides a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth is considered a PAN technology that offers fast and reliable transmission for both voice and data. Untethered Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks.

Bluetooth can be used to connect almost any device to any other device. An example is the connection between a PDA and a mobile phone. The goal of Bluetooth is to connect disparate devices (PDAs, cell phones, printers, faxes, etc.) together wirelessly in a small environment such as an office or home. According to the leading proponents of the technology (Ericsson, Intel, IBM, and Nokia), Bluetooth is a standard that will ultimately—

Eliminate wires and cables between both stationary and mobile devices

Facilitate both data and voice communications

Offer the possibility of ad hoc networks and deliver synchronicity between personal devices.

Bluetooth is designed to operate in the unlicensed ISM (industrial, scientific, medical applications) band that is available in most parts of the world, with variation in some locations. The characteristics of Bluetooth are summarized in Table 8-1. Bluetooth-enabled devices will automatically (termed, “unconsciously”) locate each other and form networks.

As with all ad hoc networks, Bluetooth network topologies are established on a temporary and random basis. A distinguishing feature of Bluetooth networks is the master-slave relationship maintained between the network devices.

Up to eight Bluetooth devices may be networked together in a master-slave relationship, called a piconet. In a piconet, one device is designated as the master of the network with up to seven slaves connected directly to that network. The master device controls and sets up the network (including defining the network's hopping scheme).

Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence. Although only one device may perform as the master for each network, a slave in one network can act as the master for other networks, thus creating a chain of networks. This series of piconets, often referred to as scatternets, allows several devices to be internetworked over an extended distance. This relationship also allows for a dynamic topology that may change during any given session: as a device moves toward and away from the master device in the network, the topology, and therefore the relationships of the devices in the immediate network, change.

Table 8.1. Key Characteristics of Bluetooth Technology 5

Characteristic	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS)
Frequency Band	2.4-2.45GHz (ISM band)
Hop Frequency	1.600 hop/sec
Data Rate	1Mbps (raw). Higher bit rates are anticipated
Operating Range	About 10 meters can be extended to 100 meters
Throughput	Up to 720 kbps
Positive Aspects	No wires and cables for many interfaces. Ability to penetrate walls and other obstacles. Costs are decreasing with a \$5 cost projected. Low power and minimal hardware
Negative Aspects	Possibility for interference with other ISM band Technologies. Relatively low data rates

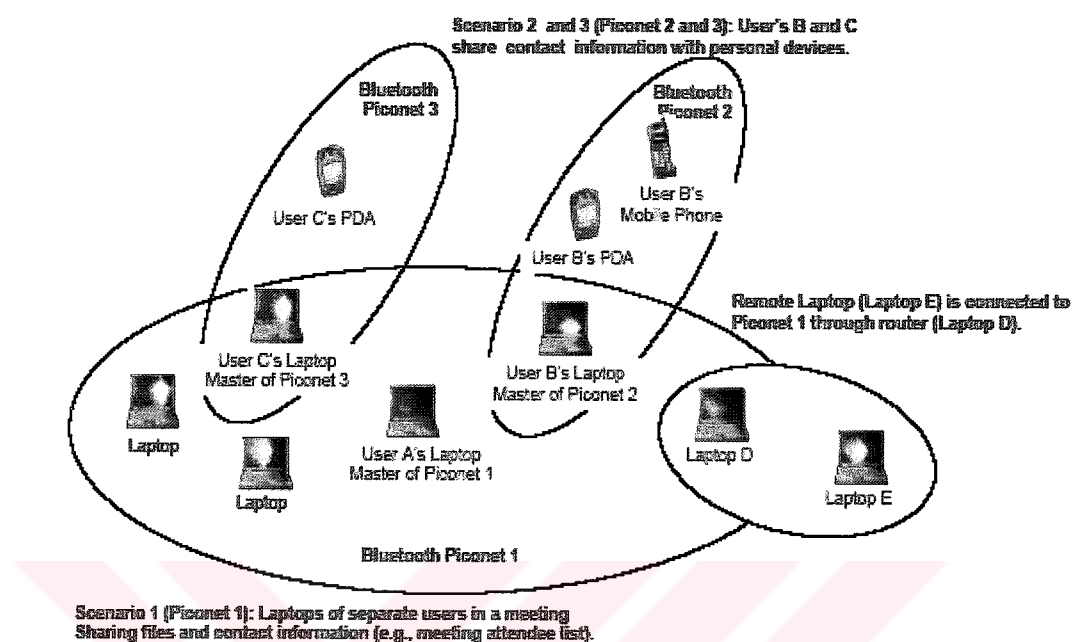


Figure 8.1. Typical Bluetooth Network —A Scatternet

Mobile routers in a Bluetooth network control the changing network topologies of these networks. The routers also control the flow of data between devices that are capable of supporting a direct link to each other. As devices move about in a random fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing protocols it employs allow Bluetooth to establish and maintain these shifting networks.

Bluetooth transceivers operate in the 2.4GHz, ISM band, which is similar to the band WLAN devices and other IEEE 802.11-compliant devices occupy. Bluetooth transceivers, which use Gaussian Frequency Shift Keying (GFSK) modulation, employ a frequency hopping (FH) spread spectrum system with a hopping pattern of 1,600 times per second over 79 frequencies in a quasi-random fashion. The theoretical maximum bandwidth of a Bluetooth network is 1Mbps.

However, in reality the networks cannot support such data rates because of forward error correction (FEC). The second generation of Bluetooth technology is expected to provide up to 2Mbps maximum bandwidth.

Bluetooth networks can support either one asynchronous data channel with up to three simultaneous synchronous speech channels or one channel that transfers asynchronous data and synchronous speech simultaneously.

Bluetooth uses a combination of packet- and circuit-switching technologies. The advantage of using packet switching in Bluetooth is that it allows devices to route multiple packets of information by the same data path. Since this method does not consume all the resources on a data path, it becomes easier for remote devices to maintain data flow throughout a scatternet.

8.1.1 Bluetooth Architecture and Components

As with the IEEE 802.11b standard, Bluetooth permits devices to establish either P2P networks or networks based on fixed access points with which mobile nodes can communicate. For the purposes of this document, however, we will discuss the ad hoc network topology only. This topology is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be internetworked without access to the wired LAN (infrastructure network). The basic Bluetooth topology is depicted in Figure 8.2. As shown in this piconet, one of the devices would be a master and the other two devices would be slaves.

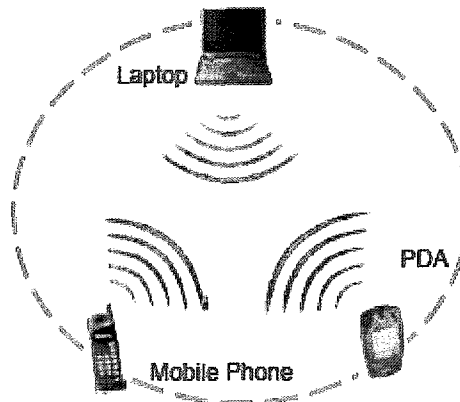


Figure 8.2. Bluetooth Ad Hoc Topology

Unlike a WLAN that comprises both a wireless station and an access point, with Bluetooth, there are only wireless stations or clients. Again, a Bluetooth client may be a laptop, a handheld device (e.g., PDA or custom device such as a barcode scanner), desktop, or any other kind of Bluetooth-enabled device. A Bluetooth client is simply a device with a Bluetooth radio and Bluetooth software module incorporating the Bluetooth protocol stack and interfaces.

8.1.2 Frequency and Data Rates

The designers of Bluetooth like those of the 802.11b WLAN standard designed Bluetooth to operate in the unlicensed 2.4GHz–2.5GHz ISM frequency band. Because numerous other technologies also operate in this band, Bluetooth uses a frequency-hopping spread-spectrum (FHSS) technology to solve interference problems. The FHSS scheme uses 79 different radio channels by changing frequency about 1,600 times per second. One channel is used in 625 microseconds followed by a hop in a pseudo-random order to another channel for another 625microsecond transmission; this process is repeated continuously. As stated previously, the ISM band has become popular for wireless communications because it is available worldwide and is unlicensed.

In the ISM band, Bluetooth technology permits transmission speeds of up to 1Mbps and achieves a throughput of approximately 720kbps. Although the data rates are low compared to 802.11b wireless LANs, it is still three to eight times the average speed of parallel and serial ports, respectively. This rate is adequately fast for many of the applications for which Bluetooth was conceived. Moreover, it is anticipated that even faster data rates will be available in future.

8.1.3 Range

As shown in Table 4-2, Bluetooth provides one of three classes of power management. Class 3 devices operate at 1 milliwatt (mW) and have an operating range of 0.1 meter to 10 meters (m). Class 2 devices operate at 10mW and have an operating range of 10m. Class 1 devices operate at 100mW and have an operating range of up to 100m.

Table 8.2. Device Classes of Power Management

Type	Power Level	Operating Range
Class 3 Devices	100mW	Up to 100 meters
Class 2 Devices	10mW	Up to 10 meters
Class 1 Devices	1mW	0.1-10 meters

The three ranges for Bluetooth are depicted in Figure 8.3. As shown, the shortest range may be good for applications such as cable replacement (e.g., mouse or keyboard), file synchronization, or business card exchange. The high-powered range can reach distances of 100m, or about 300ft. At this relatively long range, Bluetooth can compete with other WLAN technologies and applications. Additionally, as with the data rates, it is anticipated that even greater distances will be achieved in the future.

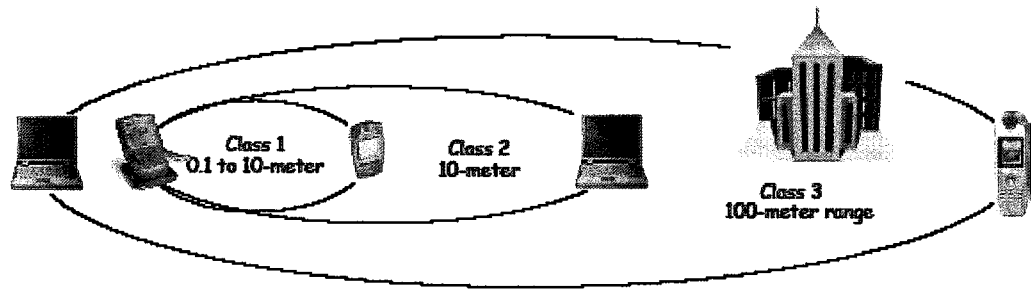


Figure 8.3. Bluetooth Operating Range

8.2 Benefits

Bluetooth offers five primary benefits to users. This ad hoc method of untethered communication makes Bluetooth very attractive today and can result in increased efficiency and reduced costs. The efficiencies and cost savings are attractive for the home user and the enterprise business user.

Benefits of Bluetooth include—

Cable replacement—Bluetooth technology replaces cables for a variety of interconnections. These include peripheral devices (i.e., mouse and keyboard computer connections), USB – at 12Mbps (USB 1.1) up to 480Mbps (USB 2.0); printers and modems, usually at 4Mbps; and wireless headsets and microphones that interface with PCs or mobile phones.

Ease of file sharing—Bluetooth enables file sharing between Bluetooth-enabled devices. For example, participants of a meeting with Bluetooth-compatible laptops can share files with each other. In another example, a Bluetooth-compatible mobile phone acts as a wireless modem for laptops.

Using Bluetooth, the laptop interfaces with the cell phone, which in turn connects to a network, thus giving the laptop a full range of networking capabilities without the need of an electrical interface for the laptop-to-mobile phone connection

Wireless synchronization—Bluetooth provides automatic wireless synchronization with other Bluetooth-enabled devices. For example, personal information contained in address books and date books can be synchronized between PDAs, laptops, mobile phones, and other devices. The synchronization occurs automatically, without the need of input from the device owner. It automatically occurs whenever the devices come within range of one another's device transmission, without the device user's knowledge.

Automated wireless applications—Bluetooth supports automatic wireless application functions. Unlike synchronization, which typically occurs locally, automatic wireless applications interface with the LAN and Internet. For example, an individual working offline on e-mails might be outside of their regular service area—on a flight, for instance.

To e-mail the files queued in the inbox of the laptop, the individual, once back in a service area (i.e., having landed), would activate a mobile phone or any another device capable of connecting to a network. The laptop would then automatically initiate a network join by using the phone as a modem and automatically send the e-mails after the individual logs on.

Internet connectivity—Bluetooth is supported by a variety of devices and applications. Some of these devices include mobile phones, PDAs, laptops, desktops, and fixed telephones. Internet connectivity is possible when these devices and technologies join together to use each other's capabilities. For example, a laptop, using a Bluetooth connection, can request a mobile phone to establish a dial-up connection; the laptop can then access the Internet through that connection.

With all of these benefits, Bluetooth is expected to be built into office appliances (e.g., PCs, faxes, printers, laptops), communication appliances (e.g., cell phones, handsets, pagers, headsets), and home appliances (DVD players, cameras, refrigerators, microwave ovens). Applications for Bluetooth also include vending machines, banking, and other electronic payment systems; wireless office and conference rooms; smart home; and in-vehicle communications and parking.

8.3 Bluetooth Security Architecture

Security can be defined by four fundamental elements: availability, access, integrity, and confidentiality. The Security Expert Group (BSEG) provides the Bluetooth SIG and associated working groups with expertise regarding all aspects of Bluetooth Security.

The current Bluetooth Specification defines security at the link level. Application-level security is not specified, allowing application developers the flexibility to select the most appropriate security mechanisms for their particular application. The Bluetooth security architecture, as specified by SIG, includes provisions for authentication and encryption. (WEB_9. 2004)

8.3.1 Security Modes

There are three security modes under which protocols can operate. A Bluetooth device can operate in only security mode at a time.

Security Mode 1 (non-secure): A device will not initiate any security procedure.

Security Mode 2 (service-level enforced security): A device does not initiate security procedures before channel establishment. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel.

Security Mode 3 (link level enforced security): A device initiates security procedures before the link set-up.

8.3.2 Security Levels

In addition to three security modes, it is possible to define different security levels for devices and services. For devices two trust levels are distinguished:

Trusted Device: Devices that have been previously authenticated, and are marked in the database as trusted. These are the devices with fixed relationship (paired) that is trusted and has unrestricted access to all services for which the trust relationship has been set.

Untrusted Device: Devices that have been previously authenticated, but not marked as trusted in the device database. These are the devices with no permanent fixed relationship (but possibly a temporary one) or device that has a fixed relationship, but is not considered as trusted. The access to services is restricted.

Unknown Device: If no security information is available for this device in the device database. This is also an untrusted device.

For services the requirement for authorization, authentication and encryption are set independently. The access requirements allow defining three security levels:

Services that require authorization and authentication: Automatic access is only granted to trusted devices. Other devices need a manual authorization.

Services that require authentication only: Authorization is not necessary.

Services open to all devices: authentication is not required, no access approval required before service access is granted.

8.4 The Bluetooth Protocol Stack

Bluetooth protocol stack can be compared with OSI model.

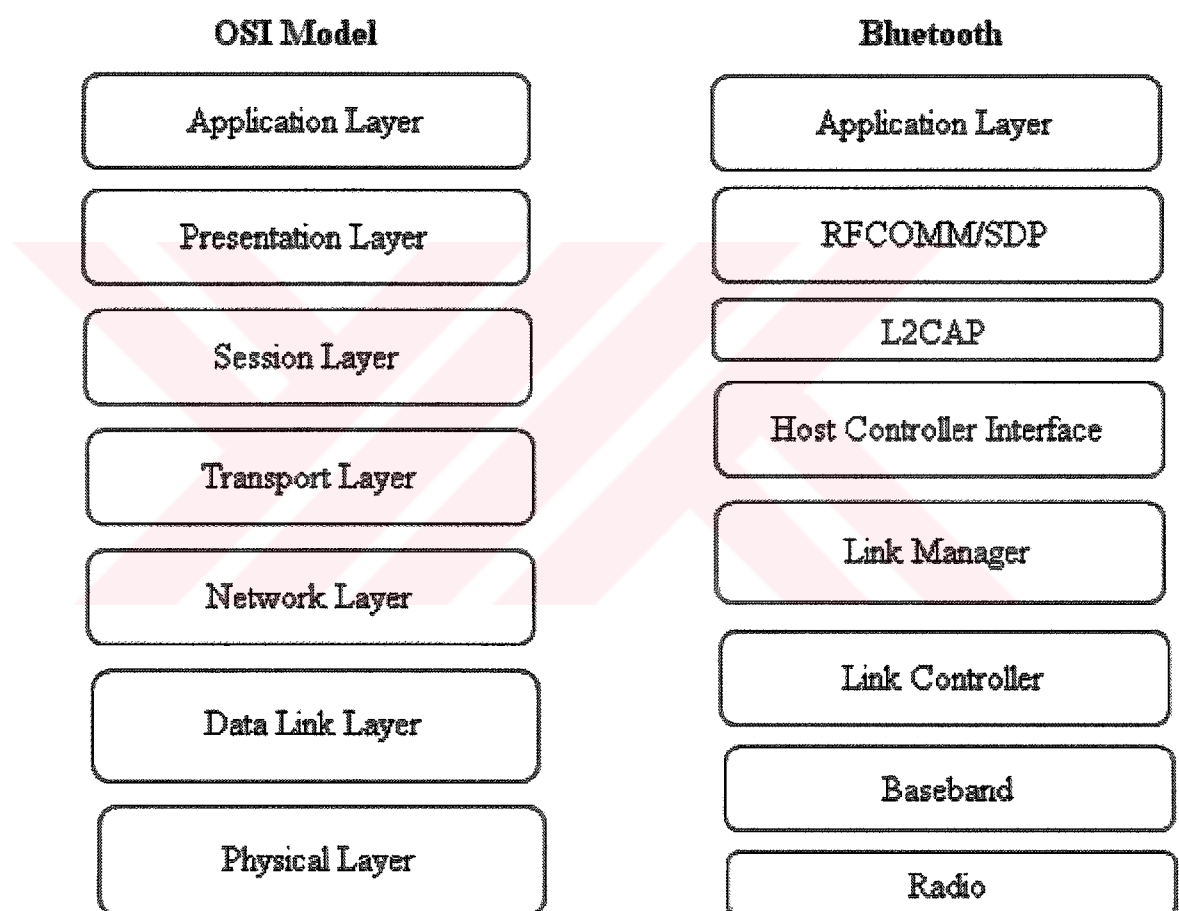


Figure 8.4 Bluetooth Stack

Physical Layer: Radio and Baseband Layers of Bluetooth stack are responsible for physical characteristics of medium.

Data Link Layer: Link controller protocol provides transmission, framing and error control over a particular link.

Network Layer: Link Manager (LM) handles data transfer across the network independent of the media and network topology.

Transport Layer: High end of Link Manager and Host Controller Interface (HCI) provides multiplexing of data transferred across network.

Session Layer: Logical Link Control and Adaptation Protocol (L2CAP) and the lower ends of RFCOMM/SDP supplies management and data flow control services.

Presentation Layer: RFCOMM/SDP provides a common representation for application layer data by adding service structure to the data units.

Application Layer: Manages communication between host applications.

8.4.1 Security Functions at Bluetooth Protocol Layers

Different security functions are provided at various layers in Bluetooth stack

Baseband Layer: Frequency hopping is one the function present at Baseband layer to provide security. Although in military application frequency hopping is used to avoid signal jamming attack, but in Bluetooth it provides less security due to the openness of the ad hoc networking model. It is also ineffective in preventing denial-of-service attacks, which can be done by flooding the ISM band with interference.

Service Discovery Protocol Layer: Bluetooth devices discover the availability of services and methods of accessing the connection at SDP. It allows user to specify how available they want to be. Thus by managing availability protects users from attacks.

Link Layer: The link layer specifies two security modes at the link level to provide protection against intrusions such as interception of broadcast signal or spoofing of incoming transmission.

One way to provide security is frequency hopping. Using its internal clock, the master unit determines the hopping scheme to be used for the duration of the Piconet. Whenever a Piconet is first formed or joined, slave devices determine the value the master clock. Using the difference between that clock and their own as an offset, they can apply the algorithm in the Bluetooth Frequency Selection Module to calculate the net's frequency-hopping sequence and change frequencies accordingly. This scheme blocks illicit listening devices that are not part of the Piconet from obtaining any significant part of the data stream on an uninterrupted basis. Other security feature is Channel Establishment. When two devices want to communicate link manager requests establishment of a link-level connection. For security mode 1 or 3, a L2CAP connection is created without further queries and channel establishment is complete. For security mode 2, the security database is queried to see if the device is authorized for access. If not, the device is rejected and the process ends.

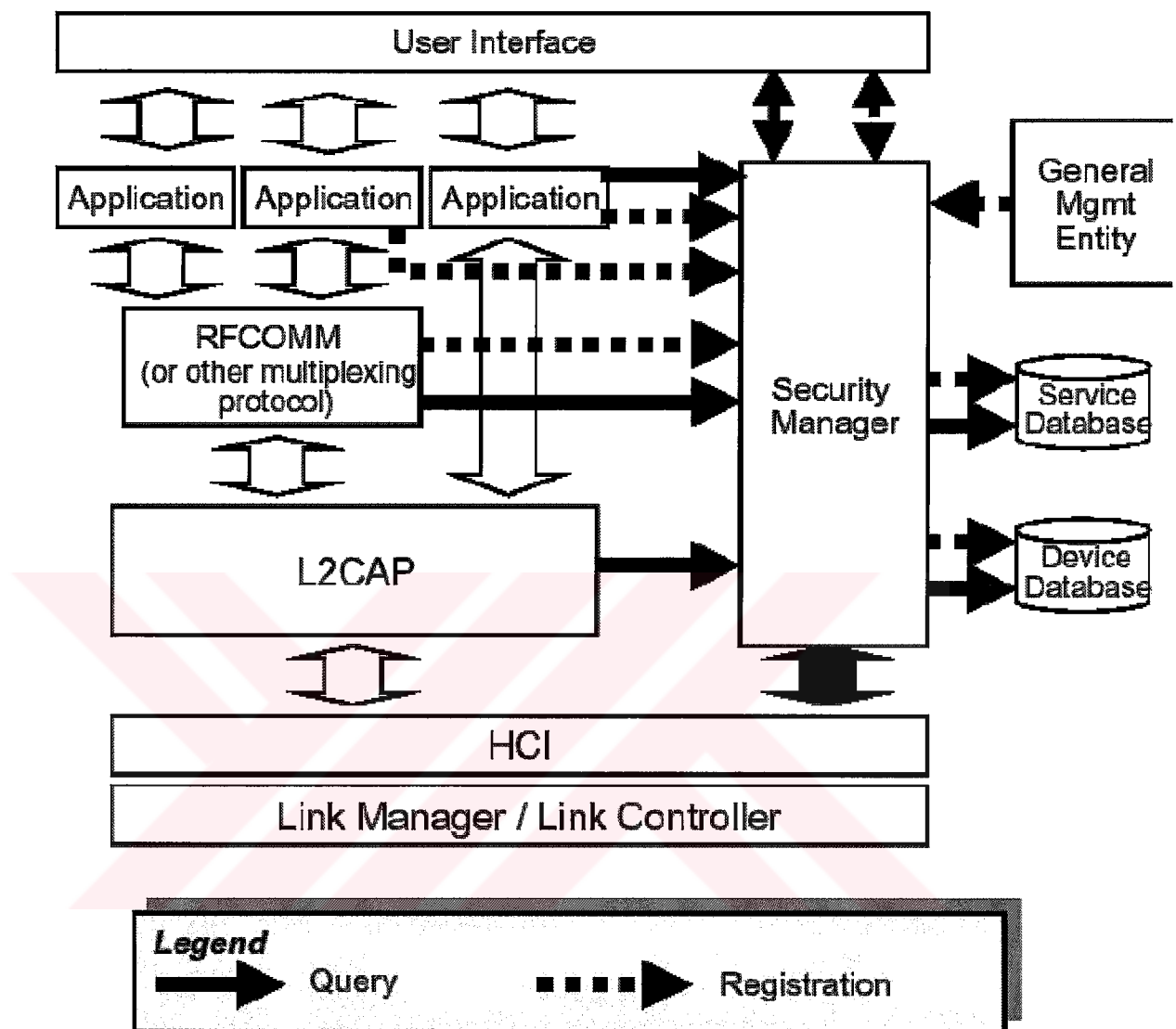


Figure 8.5 Bluetooth Security Architecture

8.5 Security Manager

Security policies are administered by exchanging queries with the security manager. The security manager performs the following functions:

- Stores security-related service information
- Stores security-related device information
- Answers access requests by protocol implementation or applications
- Enforces Authentication and/or Encryption before connecting to the application
- Initiates or processes input from External Security Control Entities, such as devices users or applications, to set up trusted relationships on the device level.
- Initiates pairing and query PIN entries by the user.
- Answers access requests from protocol layers.
- Answers HCI queries on whether to apply authentication and/or encryption to a connection.

8.6 Authentication

In a Piconet all devices are properly identified to each other. Authentication can be done using Unit keys. A unit that uses a unit key is only able to use one key for all its secure connections.

Hence, it has to share this key with all other units that it trusts. Consequently all trusted devices are able to eavesdrop on any traffic based on this key. A trusted unit that has been modified or tampered with could also be able to impersonate the unit distributing the unit key. Thus, when using a unit key there is no protection against attacks from trusted devices.

To establish a Bluetooth security of a Bluetooth transmission four elements are required.

- A 48-bit unique device address
- A 128-bit pseudo-random number private key used for authentication
- An 8-128 bit private key used for encryption
- A 128-bit pseudo random number generated by the device

Authorization process continues as follow:

1. A verifying unit sends a PDU containing a random number to the claimant unit.
2. The claimant returns an answer containing an encrypted version of the random number, its own Bluetooth Device Address, and a secret key.
3. If the response is as expected by the verifying device, the claimant is considered authenticated. Optionally the devices may switch roles and whole process will be repeated in reverse.

In case of authentication failure, a certain amount of delay is introduced before other attempt can be made. This prevents an intruder from simply trying a large number of keys in an effort to gain entry to the network. A variant of SAFER+ cipher is used in Bluetooth to perform authentication of any devices present. SAFER+ generates 128-bit cipher keys from a 128-bit plaintext input. The key may also be generated using the PIN of the device as a seed.

8.7 Encryption

A device must undergo the authentication process before starting encrypted communication. The key generated through this authentication process is used to request for an encryption mode.

There can be three different encryption modes

- ☐ No encryption
- ☐ Only point-to-point traffic is encrypted
- ☐ Both broadcast and point-to-point traffic is encrypted

The master and slave must agree on the mode of encryption to use. The master device sends the request to slave device proposing an encryption mode. If slave rejects the request, master device try again with proposal of different encryption mode.

Next step is to choose the key length. Master device send the request with a proposed key length. The key length may vary from 8 bits to 128 bits. Initially this key length is the maximum allowable length. If the slave cannot handle the key length, then master proposes a shorter key length. If two devices are unable to reach an agreement, the negotiation is aborted and encryption cannot be initialized.

For confidentiality Bluetooth uses E0, which is 128-bit symmetric cipher. Enciphering is done in three steps.

1. A payload key is generated using the Encryption key (K_c), the Bluetooth Device Address, the Clock and a Random number.
2. A key stream is generated using a series of four linear feedback shift registers.
3. Ciphertext is generated by XORING the Plaintext with Key stream. Or the Plaintext can be generated by XORING the Ciphertext with Key stream.

The cipher is vulnerable to divide-and-conquer attack in certain circumstances, vulnerability has been addressed by the re-synchronization of the cipher after each packet is transmitted or received.

8.8 Risks and Limitations

The Bluetooth security architecture has the following risks and limitations.

1. The legacy applications do not make calls to the security manager.

Instead a Bluetoothaware adapter application is required to make security-related calls to the Bluetooth security manager on behalf of the legacy application. This lack of required encryption potentially leaves user transmissions in the clear.

2. Only a device is authenticated and not its user. If there is a need for authentication of the user, other means – e.g., application level security features – will be necessary. A stolen device can be used in a malicious way by an attacker.

3. If there are two Bluetooth devices (e.g., PDAs), each having a set of applications: calendar, file synchronization, etc. The two devices will communicate, over a Bluetooth link, to perform a certain task such as file synchronization. There is no mechanism defined to preset authorization per service.

4. Privacy of transmissions is an issue for Bluetooth users. If a device moves into the range of a Bluetooth network, that identifier of device can be logged which then may be used to record the movement of device.

5. If an intruder records all communication during the key exchange and the first authentication between two units. He can then calculate, for each possible passkey value, the corresponding initialization key. Furthermore, for each initialization value, he can calculate the corresponding link key. Finally, for each link key value he can then check the response value for the observed challenge (or he can issue a challenge himself towards the victim device). If he finds a match, he has obtained the correct link key. Since all calculation steps have low complexity, unless the passkey space is large, the intruder can easily compute the correct link key.

CHAPTER NINE

HANDHELD DEVICE

9. Handheld Device Security

Today, wide ranges of devices use the 802.11 or Bluetooth wireless technology. Handheld devices, such as personal digital assistants (PDAs) and smart phones, are used in nearly every business and for private purposes. They have the power to support enterprise applications and are increasingly connected to the enterprise via high-speed wireless networks such as 802.11a/b. (WEB_10. 2004)

According to Gartner, phones and PDAs with mobile connectivity will exceed one billion units this year. There are many security threats and vulnerabilities associated with these devices. The use of handheld devices brings in new security risks to companies' existing network. To a greater extent, these devices are having their own IP addresses and can become targets of an attack. As handheld devices begin supporting more networking capabilities, network administrators must carefully assess the risks they introduce into their existing computing environment. Both device manufacturer and operating system provider have to provide some security in standard offering.

The other advanced security features should be left if not necessary, not to be burden to the handheld resources. On the other hand a business level security requires specific knowledge about specific business setup.

The businesses need to implement their own security measures (encryption, authentication etc.) by using either software applications or hardware. In the following sections we will describe how the security requirements for confidentiality, integrity, authenticity, and availability for handheld device computing environments can be endangered.

9.1 Integrity Concerns

The loss of data integrity on the handheld device represents a great security threat. Third party should be able to verify that the content of a message has not been altered in transfer and that the origin or the receipt of a specific message be verifiable by a third party. The integrity of the data can be compromised in two places, in the transport phase or while sitting on the handheld device.

One of the best ways to protect the data integrity on the handhelds in wireless environment is usage of PKI. Public/Private Key method can be used to encrypt data and messages while transferring it over the WLAN. Another way to ensure the data integrity is usage of VPN and firewalls. Nowadays, PDAs and cellular phones offer support for personal firewall and usage of the VPN in order to prevent the data integrity.

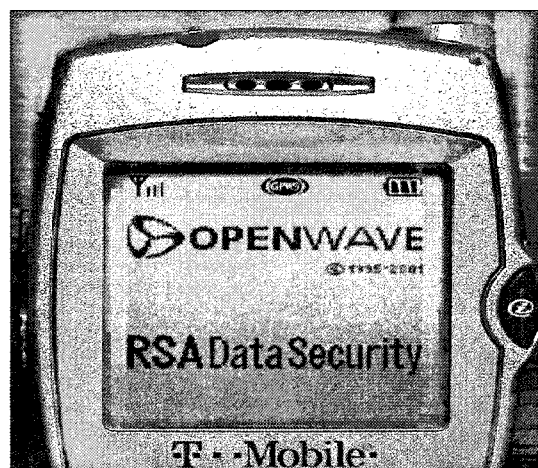


Figure 9.1 RSA

9.2 Availability Concerns

The major concern for the users of handhelds, beside the information integrity data, is availability of devices. As mentioned before, many of the handheld devices have IP address assigned to them, which leaves them susceptible to DoS attacks. As a result of this attack the devices become unavailable to other network devices. The counter measures for DoS type of attacks are the same as for other wireless stations in the WLAN environment, such as special functions within firewalls and monitoring of the pre-established thresholds for packet floods.

9.3 Confidentiality Concerns

The most essential security requirement for every company is the confidentiality of data. Due to the broadcast and radio nature of wireless technology, confidentiality is a more difficult security requirement to meet in a WLAN. Great majority of the handhelds is shipped with already enabled wireless connectivity and the default settings in most cases do not match the security policies established in companies. The rogue handhelds can try to access other WLAN enabled devices (other PDAs, laptops etc.). On the other side, compromised workstations can try to establish links with PDAs. Many handhelds today come with integral modems, which enable them to dial-in to companies' facilities and access the internal network using loopholes. If one company make use of handhelds in its environment, it is likely that handhelds will communicate with other devices (servers, workstations etc.) around them. An 802.11-enabled device with no security/encryption in place can expose data to other 802.11-enabled devices. Without proper confidentiality measures implemented, a rogue handheld device can attempt to synchronize with workstations around it, and access valuable data. One of the countermeasures that enterprises can employ to prevent the loss of the data and ensure the confidentiality is forbidding the usage of wireless-enabled PDAs in corporate facilities.

Other measures include implementation of some sort of encryption on handhelds by using either software or hardware. Other possible attacks can come by using IrDA, Bluetooth or analog phones.

For instance analog phone conversations can be intercepted by using relatively simple radio scanners. Alternative to use of the analog phones are digital spread spectrum telephone technology. They use pseudo-random code sequences and some forms of encryption.



CONCLUSIONS

Security is a very difficult topic. Everyone has a different idea of what "security" is, and what levels of risk are acceptable. The key for building a secure network is to *define what security means to your organization* . Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

Many people pay great amounts of lip service to security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know *why* what's been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them.

Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

As a result of securing of wireless and non-wireless, you should do the following these steps

1) Don't use TCP/IP for File and Printer sharing!

Access Points are usually installed on your LAN, **behind any router or firewall you may be using**. If someone successfully connects to your Access Point, they'll be on your LAN, just like any of your other clients. But since they'll be using TCP/IP to make the connection, you can easily deny access to MS File and Printer sharing by using a protocol other than TCP/IP for those services. That way, they may get access to your Internet connection, but they won't get access to your files

2) Follow secure file-sharing practices

This means:

- Share only what you need to share (think Folders, not entire hard drives)
- Password protect **anything** that is shared with a **strong password**.

3) Enable WEP Encryption

802.11b's WEP encryption has had a lot of bad press lately about its weaknesses. But a weak lock is better than no lock at all, so **enable WEP encryption** and use a **non-obvious encryption key**. Look for and use products that support 128bit WEP. Prices have come down on 802.11b equipment so there's no need to buy something that doesn't support 128bit WEP.

4) Use WEP for data and Authentication

Some products allow you to separately set the Authentication method to "Shared Key" or "Open System". Use the "Shared Key" method so that encryption is used to both authenticate your client **and** encrypt its data.

5) Use non-obvious WEP keys and periodically change them

While the limitations that some wireless client utilities have don't help (hexadecimal only support, single keys, forgetting keys, etc.), don't make it easy for potential snoops to get onto your LAN by using simple keys like 123456, all ones, etc. Changing the keys periodically is more difficult, because it requires sending out information about the new keys to users and that can be a security problem in itself. But changing keys periodically can help keep your LAN secure, so consider getting a procedure into place to do it.

6) Secure your wireless router / Access Point (AP)

Your router or Access Point should require a password to access its Admin features. If it doesn't, **get one that will!**

7) Disallow router/ AP administration via wireless

Unfortunately, this feature is usually only present in "Enterprise-grade" APs, and shuts off the ability to administer your Access Point from wireless clients. But if your router/AP has it, use it!

8) Use MAC address based Access and Association control

Previously available only on "Enterprise-grade" products, many routers and Access Points are being upgraded to have the ability to control the clients that can use them. MAC addresses are tied to physical network adapters, so using this method requires a little coordination and maybe a little inconvenience for LAN users. And MAC addresses can be "spoofed" or imitated/copied, so it's not a guarantee of security. But it adds another hurdle for potential intruders to jump. If you already have a product that doesn't include this feature, check your Manufacturer's Web.

9) Use VPN

Of course, if you really don't want to take chances with your data, then you should run a VPN tunnel over your wireless connection, too. You may take a throughput hit, but isn't your data's security worth it?

10) Install Only the Minimal Set of Services and Applications

Either do not install unnecessary services, or turn the services off and remove the corresponding files (source, binary, executable, configuration, and data files) from the server. Be careful with network service programs. Some provide multiple services, and an administrator will have to reconfigure them or disable unnecessary services. For example, Web server software often includes FTP along with HTTP.

Disable FTP if file transfers to and from the public Web site are not required. If FTP service is required, severely restrict access to it, and carefully consider how anonymous FTP will be used.

When considering services to enable or disable, administrators typically think of those services that run as processes. For example, these include telnet, FTP, DNS, electronic mail, and Web services. However, most of today's systems also provide services directly from the kernel. An example of such a service is a netmask request. This request is typically broadcast onto the local area network, and all systems seeing this request answer it unless otherwise instructed. The kernel of those answering systems is providing the netmask service, more than likely unbeknownst to the administrator of that server.

Determine what services the kernel provides, and what controls the operating system provides to configure these services. These services are frequently not documented, and are often not controllable. There is no tool that we know of to test for the presence of

such services in a manner similar to the way the strobe tool for UNIX systems tests for services running as processes. The best source of information is the system vendor.

11) Eliminate any Unnecessary Open Network Ports

Eliminate unnecessary TCP and UDP network ports on which a server process may listen for incoming client connections. This reduces the risk of attack using these ports. Open network ports can be identified using the netstat command on UNIX and Windows systems.

12) First deny and then allow

We recommend using the configuration principle "deny first; then allow." That is, turn off as many services and applications as possible and then selectively turn on only those that are essential. We also suggest installing the most minimal operating system configuration image that meets business requirements, but realize that not all operating systems support doing so.

This practice is most effective if it is performed as part of the initial operating system installation and configuration versus retrofitting an operational server executing in a production environment.

12) Create and Record Cryptographic Checksums

After making all configuration choices, create and record cryptographic checksums or other integrity-checking baseline information for critical system software and its configuration.

REFERENCES

WEB_1. (2004) <http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/> , 10/07/2004

WEB_2. (2004) <http://www.cert.org>, 11/06/2004

WEB_3. (2004) <http://www.microsoft.com>, 09/06/2004

WEB_4. (2004) <http://www.itweek.co.uk/Features/>, 12/05/2004

WEB_5. (2004) <http://www.wi-fi.com/OpenSection/>, 05/06/2004

WEB_6. (2004) <http://www.scia.org>, 01/04/2004

WEB_7. (2004) <http://www.wirelessinternetmag.com> , 01/04/2004

WEB_8. (2004) <http://www.itsecurity.com>, 11/07/2004

WEB_9. (2004) <http://www.bluefiresecurity.com/downloads/Bluefire>, 22/06/2004

WEB_10. (2004) <http://www.informationweek.com>, 22/06/2004