PERSONAL FIREWALL IN MOBILE PHONE

by

Edina Arslanagic

Masters Thesis in
Information and Communication Technology

Agder University College
Faculty of Engineering and Science

Grimstad, May 2004

Summary

The assignment described in this master thesis is given by Ericsson AS and gives an evaluation of a need for a personal firewall in mobile phone. In today's commercial products personal firewall in mobile phone does not exist. This master thesis analyzes the role of personal firewall in different scenarios.

At the beginning of the master thesis functions that already exist in personal firewall for PC were discussed in the sense of which could be useful in personal firewall for mobile phone. This master thesis also covers description of connection between personal firewall and virus in addition to what personal firewall can do to prevent virus and other malicious software. Different types of attacks (Denial of Service, Port Scanning, IP spoofing, etc.) and what personal firewall can do to prevent such attacks were evaluated.

Mobile phone's specific functions (Billing & Charging), mobile phone standard functions (WAP/WWW) and P2P services over IP (Push-To-Talk, Buddy list and Wireless Village) need support from a personal firewall so that users feel more secure using them. Furthermore, personal firewall protection is essential regarding downloadable applications from the Internet.

Connection types: GPRS/UMTS, WLAN and Bluetooth are discussed to be vulnerable to different types of attacks. Functions in personal firewall that could prevent these attacks were outlined. Possible ways to implement personal firewall for various connection types were also suggested.

One possible way to implement personal firewall could be as software in mobile phone for all connection types. It is also possible to implement it in the GGSN and in mobile phone for GPRS and UMTS. Operators offer services in GGSN's personal firewall while user can add several rules. This implementation is best suitable for GPRS and UMTS. Personal firewall as software implemented in the mobile phone is configured by a user and suitable for all connection types.

An analysis of personal firewall implementations with their advantages and disadvantages are proposed in this master thesis. Discussion on different layers in mobile phone and what underlying functionality mobile phone must provide to get a working personal firewall was also covered.

Aspect of packets filtering has also been evaluated: network filtering, filtering in personal firewall and application level filtering. If filtering is done in IP layer, it is fast and less secure comparing to application level filtering. IP filtering is based on the header information, while application level filtering is based on content of the whole packet. Filtering in personal firewall includes a part of IP stack responsible for filtering.

I have found that the need for personal firewall in mobile phone with proposed useful functions is essential. Even though implementation of personal firewall could be difficult, it is better then no protection at all.

Preface

This master thesis is a part of the Master of Engineering degree in Information and Communication Technology at the Agder University College, Faculty of Engineering and Science in Grimstad. This assignment is a closure on the education that leads to the Norwegian degree Sivilingeniør, which is equivalent to a Master of Science degree. The work has been carried out in the period between January 2004 and May 2004.

The assignment is given by Ericsson AS and gives a theoretical evaluation on the need for personal firewall in mobile phone. It has been a comprehensive and challenging task to complete this thesis, and it has required a lot of information collection and understanding.

This research work is based on co-operation with Harald Johansen (Master of Science) who provided information and knowledge about the theoretical part of the assignment. I would like to take the opportunity to thank Harald Johansen for his time and interchanging ideas and solutions.

And finally I would like to thank my supervisor at HiA, Geir Køien for helping with the administrative part of the thesis.

Grimstad
Spring 2004

_____
Edina Arslanagic

Table of contents

List of figures

List of tables

"Security is a chain; it's only as secure as the weakest link. Security is a process, not a product."

"This is obvious anyone involved in real-world security. In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process. And if we're going to make our digital system secure, we're going to have to start building processes."

Secrets & Lies

Digital Security in a Networked World

Bruce Schneier

1 Introduction

This chapter gives an overview of the background for master thesis, task definition and limitation of the thesis.

1.1 Background

The number of mobile phone users that use Internet connection has faced a massive growth during the last years. There is a reason to believe that these numbers will continue to grow during the next years, since Internet has become more and more popular among all groups of users.

An always-on Internet connection is a tempting target for an attacker. Dial-up connections are hard for attackers to use effectively: they are slow and usually brief, and the connection's IP address is different each time for a call. Because IP address does not change (or changes only rarely), fast permanent connection to the Internet is quite attractive: the attacker can return to the computer or mobile phone again and again.

Mobile phones became more vulnerable to attacks since Internet connection is available on mobile phone. Some attackers just want to make life hard, look through the files for personal information or crash the mobile phone. Others might be looking for a way to use other mobile phone's account or just inflect mobile phone with a virus. Permanent high-speed connections make all of these possible for malicious attackers.

From the security point of view, the most important thing regarding PCs and mobile phones is to protect and prevent these from being attacked or inflected by insecure content. The task of preventing from attacks could be expensive and could imply a lot of resources. To implement firewall as a barrier between trusted and untrusted networks would improve security significantly. Firewall is a good solution for big companies that need high-level protection. Single users do not need the same high-level protection; they need a simple, reliable and if possible low-cost protection, namely; ***personal firewall***. Having personal firewall users would feel more secure in using their PC or mobile phone. In addition, it would be much more difficult for a hacker to attack or gain access and destroy sensitive data.

In today's commercial products personal firewall in mobile phone does not exist. In these days there are some secure software build in phones that already secure Internet connection. The need for personal firewall in mobile phone becomes essential, especially during the Internet connectivity and downloading Java applications. In addition, there are mobile phone functions (e.g., WAP/WWW, charging & billing) and more and more popular service (Push-To-Talk, Buddy list, etc.) that need support from personal firewall. With personal firewall, users will feel more secure to use these services and functions.

1.2 Thesis definition

This assignment is given by Ericsson AS and gives an analysis of the aspects of security issues in a mobile phone, emphasizing the need for a personal firewall in mobile phone. Evaluation of how personal firewall could be implemented in the mobile phone and aspect of packet filtering are also discussed.

A proposal on which personal firewall functions for PC that could be useful in mobile phone's personal firewall will be discussed in this master thesis. The essence of the master thesis is a need for personal firewall in mobile phone, relating to the mobile phone functions and P2P services that need support from the personal firewall. Vulnerability to attacks from the network should be emphasized in this master thesis, with a closer look to the connection between personal firewall and virus.

The assignment is mainly a theoretical evaluation and the following issues will be outlined:

- Useful functions in personal firewall for mobile phone
- Connection between personal firewall and virus
- Vulnerability to attacks from the network
- What support from a personal firewall is needed for standard, specific mobile phone functions and mobile phone services over IP
- Security issues, regarding downloadable applications (e.g., java programs and games)
- Discussion on various connection types (WLAN, Bluetooth, GPRS, UMTS, Internet and Intranet)
- Possible ways to implement personal firewall and aspects of filtering will also be discussed and proposed.
- Proposal of what underlying functionality the mobile phone must provide in order to get a working personal firewall.

Complete master thesis should be seen in a context of what already exists in IP security functions in the whole chain: from mobile phone to the service provider.

1.3 Limitation of the thesis

This maser thesis will deal with the attacks from the network on a mobile phone. While a traditional personal firewall protects internal users from external users, it does nothing to protect or isolate internal users from each other. This phenomenon is best known as insider attack. Insider attacks, such as stealing a mobile phone and using it without user's knowledge or changing PIN code, will not be taken into consideration in this master thesis. Also, the description of malicious software (e.g., virus) will only be seen in the context of personal firewall regarding mobile phone. The discussion will be limited to possible virus related attacks on mobile phone. Antivirus protection will thou be introduced briefly.

2 Firewall overview

This chapter deals with definition of firewall and what types of firewall exist. It outlines functions that already exist in commercial personal firewall products for PC. Furthermore, it defines personal firewall. It also gives a suggestion which of these functions could be useful in a mobile phone.

2.1 What is a firewall?

The term firewall has been around for quite some time and originally was used to define a barrier constructed to prevent the spread of fire from one part of building or structure to another. Network firewalls provide a barrier between networks that prevent or deny unwanted or unauthorized traffic.

There is no single agreed-upon definition for a network firewall. In recent years, many definitions have been developed and used. The definitions may be worded differently, but they all exhibit characteristic common theme.

A firewall is a computer, router or other communication device that filters access to the protected network [1]. Main functions of the firewall are:

- All traffic from inside to outside, and vice-versa, must pass through it.
- Only authorized traffic is allowed to pass through it.
- The firewall itself is immune to penetration.

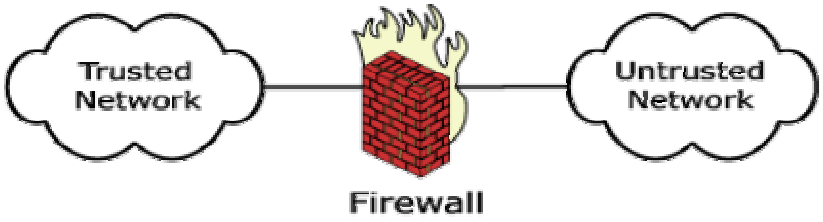


Figure 2.1 Network Firewall Illustration

Firewalls can be composed of a single router, multiple routers, a single host system or multiple hosts running firewall software, hardware appliances specifically designed to provide firewall services, or any combination thereof. They vary greatly in design, functionality, architecture, and cost.

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. A Firewall in its most simplistic sense controls the flow of traffic. It may be a hardware device (Figure 2.2) or a software program running on a secure host computer (Figure 2.3). In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to, as illustrated in Figure 2.1. A firewall sits at the

junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers [2].

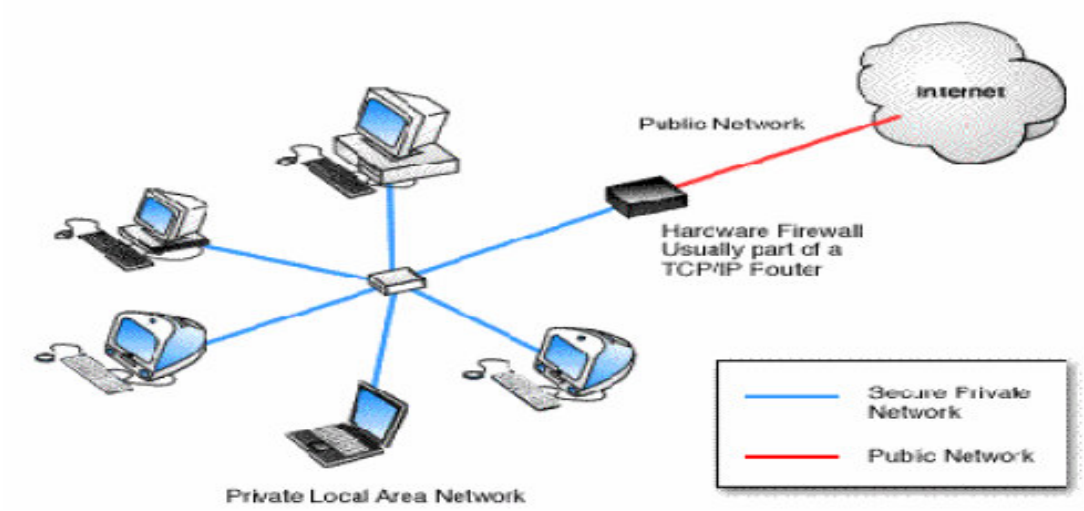


Figure 2.2 Hardware Firewall providing protection

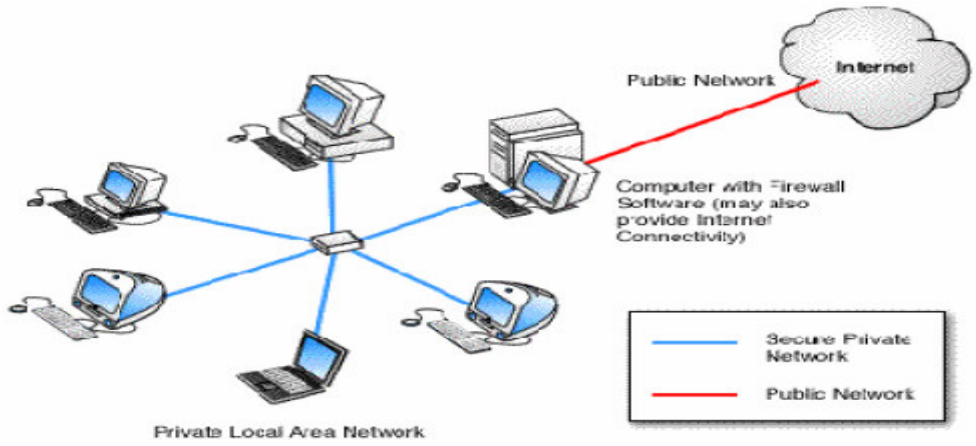


Figure 2.3 Computer running firewall software to provide protection

2.1.1 Functions of Firewall

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks; otherwise it is stopped. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers, called address filtering. Firewalls can also filter specific types of network traffic. This is known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, FTP or telnet. Firewalls can also filter traffic by packet attribute or state.

2.2 Types of firewalls

A firewall's security design logic is enforced using some type of packet-screening method. These methods are based on how firewalls use pre-configured rules, filters and information gathered from packets and sessions to determine whether to allow or deny traffic. The three well-known methods are: packet filtering, proxy based filtering and stateful packet inspection.

Filter based firewalls filter packets based on: source and destination IP addresses and TCP/UDP source and destination port number. Since only header information is checked this method of filtering is fast and has little impact on network performance. In addition, it is important to mention that packet filtering is application independent since filtering is based on header's information and not on information that relates to a specific application. On contrary, this method is less secure since it can leave open ports to all traffic passing trough that port. Unfortunately, packet filtering is vulnerable to certain attacks: IP spoofing, buffer overruns and ICMP tunneling.

Proxy-based firewalls are implemented on a secure host system configured with two network interfaces. The proxy acts as an intermediary between two endpoints. The client/server model is broken since it does not allow a direct communication between endpoints. In turn it keeps internal and external networks separate. These firewalls filter the whole packet and are therefore more secure. Filtering of whole packets may have negative impact on performance since traffic passes through all layers until it reaches application layer where they are inspected.

Stateful packet inspection examines packet header information from the network layer to the application layer, seen in the content OSI model. Arriving packets are then compared to pre-configured rules in firewall and based on this comparison packets are either allowed or denied. This method of filtering has little impact on network performance and is secure since filtering goes deeper into header information. Client/server model is not broken and therefore a direct communication between two endpoints is allowed.

For more details on types of firewalls with their strengths and weaknesses, see Appendix A [1].

2.2.1 Who needs a (personal) firewall?

Firewall is an important factor in securing PC from being attacked or influenced by insecure content. In other words, firewall is essential part of defense mechanism regarding security. Everyone, from big companies to an ordinary user, should be aware of possible harms when connected to Internet and everyone should be encouraged to use (personal) firewall.

Everyone connected to the Internet should use firewall. It should give protection against malicious software and possible attacks from the network. To give best protection personal firewall should include useful functions discussed later in this chapter.

2.3 Firewall vs. Personal Firewall

Technology commonly called “firewall” and marketed as security provider for a network is personal firewall. Personal firewall provides protection to a single device (e.g., personal computer) from untrusted network (e.g., the Internet). Again, comparing to the firewall definition, personal firewalls do not meet the criteria for already described term of firewall. Personal firewalls do not control access between two networks; **they control access to one specific device** [4]**.**

Personal firewall is a computer with the ability to filter its incoming and outgoing traffic and it is important in protecting PC from being attacked or inflected by insecure content. Just like firewall, personal firewall is a piece of software or hardware and its responsibility is to protect machine it is installed on. All outgoing and incoming traffic should pass through personal firewall and all packets are filtered in personal firewall.

The “perfect” personal firewall would be inexpensive and easy to install and use. The main functions of personal firewall would be:

- Offer clearly explained configuration options
- Filtering of outgoing/incoming traffic
- Hide all ports to make system invisible to scan
- Protect the system from attacks
- Track potential and actual threats
- Immediately alert user to serious attacks
- Ensure nothing unauthorized entered or left system

Personal firewall can be post-configured by user, in addition to already offered functions in personal firewall. User sets rules in personal firewall for handling of traffic. Based on these sets of rule, personal firewall can deny (e.g., it does not trust location traffic comes from) or allow (e.g., traffic address matches rules in personal firewall) access of traffic. Functions for personal firewall for Windows PC and Linux PC will be briefly described next.

2.4 Functions in personal firewall

Functions in personal firewall listed below are functions that already exist in commercial personal firewall products for Windows [4] [5] and Linux PC [3].

2.4.1 Functions in personal firewall for Windows PC

Table 2.1 Functions in personal firewall for Windows PC

Monitor incoming traffic	Personal firewall should look at all network packets coming from the Internet and allow only: • Those networks to send response to request that were sent out to the Internet. • Those packets for which user has configured rules at the firewall.
Monitor outgoing traffic	Personal firewalls have their own special version of scanning for outgoing traffic. Whereas enterprise firewalls define allowed outgoing traffic in terms of protocol, user, time of day, or addressed Web site, personal firewalls are often application-aware. They allow only outgoing traffic from applications that are on trusted application list. This is an important measure for preventing Trojan horse programs from communicating with the Internet (described in the Chapter 3). It also stops so-called *adware* or *spyware* programs that connect to their home server on the Internet to relay the list of sites the user has visited. Antivirus programs usually do not scan for these *adware* programs.
Detection intrusion attempts	Besides monitoring incoming network packets and deciding which should be allowed in or blocked, personal firewall may also go one step further and scan for patterns of network traffic that indicate a known attack intrusion attempt.
Alert the user	When something suspicious occurs during the monitoring of the incoming and outgoing network traffic or while scanning for known attack patterns, personal firewall usually alerts the user. It can be done either by displaying a dialog box or by flashing an icon. Whereas enterprise firewalls tend to concentrate on creating extensive log files, personal firewalls like to get the user into live action. Initially, it may scare the user how often the firewalls deems things important enough to warn about. Those are usually automated scripts or bots scanning the ports. In fact, this “knob ratting” may happen so often that the user do not pay attention to it anymore.

Trust(ed) site	The trust site feature increases user friendliness as it lets the user approve (trust) all active content on a site with one rule, thereby reducing the number of “warnings” that the user needs to take action one from the same site.
MAC address authentication and Trusted IPs	MAC address authentication is useful for scenarios where two or more computers are connected to a router that also assigns an individual public IP to each connected PC. By letting personal firewall know which MAC address that should be trusted, connected PCs with public IPs within the same hub may communicate with each other freely. With Trusted IPs user can add single IP address or range of addresses that user trusts and with which user wants to share services with. These functions are basically same i.e. trusted host but on different levels.
Port scan detection and logging	These events occur when a number of packets arrive at the system to different services (ports) but from the same host (source). When this pattern occurs within an interval of time, personal firewall will log this event as port scan. The purpose of port scans is to discover what services the system is providing and could be used as a preliminary investigation prior to hacking attempts on the system.
JavaScript Pop-Up blocker	With personal firewall, user is able to block or accept pop-ups that are launched using JavaScript techniques. Although, this feature will stop most pop-ups that are automatically launched, it might miss pop-ups that are launched using other techniques. User should also be aware that if some web sites use this method to launch a legitimate window, it will be stopped.
Updating function for a new version	With this function in personal firewall, new versions of software are automatically updated while being installed in the PC and checked for eventual errors.

2.4.2 Other features in personal firewall for Windows PC

Table 2.2 Other functions in personal firewall for Windows PC

Connection security	Personal firewall will monitor every application that attempts a connection to the Internet/network. Each application will be automatically assigned its own "guard" for monitoring. Applications that do not use the Internet/network are free from any kind of monitoring. Since there is no connection to the Internet/network the user does not have to worry that some applications will send out information without his knowledge. Trojans that seek to control the system from an incoming connection will be detected, as well as scripts that attempt to send e-mails using user’s

	name. User can control which peers who can view and access shared folders and even prevents others from detecting computer's presence on the network.
Collection of behavioral patterns	While being connected on Internet, snippets of information are being sent out between the browser and visited web sites. So-called "cookies" are useful for the sites to differentiate between users, but could also be collected and used to provide information about user's habits. This information such as "referrer" (the web page user came from) can also be blocked.
Active Content nuisance	Active-Xs, Java-/VB-Scripts and Java Applets are supposed to enrich the Internet experience for users. However, malicious versions of such content can cause serious security breaches. Personal firewall gives user total control over which sites that can activate such behavior on the PC, and sites that should be stopped. The banned sites are blocked by: ▪ URL address ▪ Words in the URL address ▪ Content on sites (words in a banned word list matching words found on web pages) Parents can edit this banned word list. They can e.g., enter words containing things they do not want a child to see.
Time Control and Account Manager	Parents are able to define one or more accounts with user passwords. Each account can be given a total time (may differ for each account) pr. day/week/month and/or special hours during the day.
Scans	Attackers often scan computers looking for vulnerabilities, especially the popular well-known cable modem subnets. Because incoming scans are "unsolicited" (i.e. do not match something in firewall's traffic memory), they are blocked.
File sharing and anonymous connections	Windows networking is intended to allow easy file sharing between computers; anonymous connections are used for discovering a computer's name and list of available file shares. On the Internet user does not want to do this and firewall prohibits these kinds of connections.
Logging Activity	Firewall does not display on-screen alerts when it blocks traffic. It does, however, log its activity to a file. Ordinarily firewall will log dropped packets (i.e. incoming traffic that firewall blocked).

2.4.3 Functions in personal firewall for Linux

A typical Unix/Linux firewall operates in kernel space. Most operating systems today claim to have network-filtering capabilities. In the Linux world, firewall is called *netfilter* and de facto configuration tool is called *iptables*. Firewalls in Linux are stateful packet inspection type.

Personal firewall could be set up from the scratch. It would contain of Linux system with one network interface, the running kernel with netfilter support and the IP-address of the network interface [3].

Table 2.3 Functions in personal firewall for Linux

Filtering	As network traffic passes through the firewall, it inspects every TCP/UDP/ICMP packets header. Filtering is based on the information in the header, and firewall decides what to do with it. The packets go through several stages, and filtering/routing decisions can be done on every stage.
Setting the policy for the chains: DROP	The default policy for a chain shows what will happen with packets that do not find any match. Setting the policy to ACCEPT means that user has to sort out single-handedly every type of traffic want will be dropped. Setting it to DROP is a more secure approach.
Accepting traffic that is related to an established stream	IPtables have the possibility to see what packets belong to an ongoing connection. This simplifies the rules, since it can allow related traffic from the beginning. Then, the only thing to take care of is the connection attempts.
The FORWARDING chain	Forwarding of IP packets goes through several stages. The FORWARDING chain belonging to the *filter* table is responsible for filtering all forwarded traffic.

2.5 PC vs. Mobile Phone

Personal computers have been a target for hackers for a long time. The need for firewalls and personal firewalls was present from the very beginning of the Internet era. Since the mobile phone market has exhibited extraordinary growth in 2003 and 2004, and use of games and other java applications has increased, the need for personal firewall in mobile phone becomes essential. Two years ago, mobile phones were not capable of downloading java (or any other) applications that might make them vulnerable to attacks.

New mobile phones are capable of downloading applications, such as java programs and games, and this creates a great opportunity for hackers to attack. This is one of the main reasons why there is a need for personal firewall in mobile phone. This will be described in more detail in Chapter 4.

The security of first and second generation systems is based on the traditional telecom security model (separation of user data and signaling data). The third generation mobile systems is IP-based and, at least partially, connected to the Internet. IP-networks are open networks, which do not separate signaling from the user data. This allows malicious users to exploit the faults of the protocol stacks to gain access to data or network resources. The 3G systems have to adopt a new security policy and build Internet security architecture (personal firewalls, virtual private networking, end-to-end encryption, etc.).

Next important difference between PC and mobile phone is that PC has open application Operative System (OS). Because of open application's OS nature, it is easier to attack PC. Mobile phones have a trend to become open application OS, especially regarding Symbian[1] [6] OS application signing program. This makes mobile phone more like PC i.e. mobile phones are becoming more vulnerable to malicious attacks. This applies especially mobile phone build on Windows CE. This means that mobile phone will eventually need same kind of protection as PCs have today.

[1] The industry-endorsed Symbian OS application signing program that creates wider commercial opportunities for developers and faster routs to market for mobile application.

2.6 Functions in personal firewall for mobile phone

From security point of view, mobile phone needs the same protection as PC, since the same Internet services are used in mobile phones. Attacking mobile phone could be a challenging task comparing to PC. Extraordinary growth of using and downloading applications from the Internet can increase possibility of attacking mobile phone. Functions that may be useful in personal firewall in mobile phone are listed below.

Table 2.4 Useful functions in personal firewall for mobile phone

Monitor incoming traffic, filtering and blocking	Monitor incoming traffic seems to be an important feature in personal firewall for mobile phone in the same way as for PC. Personal firewall should look at all network packets coming from the Internet and monitor these. One way of monitoring traffic is to allow only certain trusted servers to send traffic to the mobile user. This might require the servers to be authenticated and the transmission between the servers and the wireless network to be protected. In practice, WWW and WAP browsing could be supported by using a limited number of trusted proxy servers. Similarly, the access to e-mail accounts could be allowed using only trusted mail servers. If unknown servers are allowed to send traffic to mobile subscribers, personal firewall should be able to detect likely attack and react by filtering or blocking the traffic. If the malicious server manages to inflict considerable charge on the subscriber, the billing system should be able to compensate the subscribers' account to prevent the loss of trust towards the wireless service. This functionality becomes important since Internet connections (e.g., e-mail, WWW) and java applications are used in mobile phone. Such applications need filtering and eventually blocking as mentioned above.
Monitor outgoing traffic	Personal firewall should allow outgoing traffic from applications that are on trusted application list, since personal firewall is often application-aware. This is an important measure for preventing Trojan horse programs from communicating with the Internet. Some *adware* or *spyware* programs are getting smarter and know that certain personal firewall looks at the name of the application to decide whether outgoing traffic is allowed. These names could easily be renamed. This is why detecting outgoing traffic is an important feature in personal firewall, and outgoing traffic should be based on checksum of the entire application, instead of just name.

Detection intrusion attempts	Personal firewall in mobile phone can scan for patterns of network traffic that indicate a known attack intrusion attempt. The personal firewall may even have an updatable list of intrusion-detection signatures to respond to newly discovered attacks methods.
Trust site	Trust site feature could be useful in mobile phones while using the WWW. This function will warn sites that may include insecure content, such as virus. WAP is also important while speaking of trust site. Mobile users can access their mailbox (which might include virus) from WAP enabled cell phones. This is the reason why trust site could be an important feature in personal firewall in mobile phones. It could also be very useful in VPNs. A VPN is an encrypted tunnel over the Internet or another untrusted network, providing confidentiality and integrity of transmissions, and logically all hosts in a VPN are on Intranet. Personal firewall in mobile phone should include VPN capabilities (reasonable extension) to secure networks, so that they can safely communicate in private or public network. This could be achieved by strong authentication and encryption of all traffic between them.
MAC address authentication	This feature can only be useful in Bluetooth connection type, or eventually in WLAN in future. It is used for authentication where two or several mobile phones are connected to the same platform. Mobile phones are authenticated with the MAC addresses.
Port scan detection and logging	Port scanning and logging in mobile phone work at the same principal as for the PC, accept for one difference. It costs to send packets, which are blocked in return from mobile phones.
Active Content nuisance	Active-Xs, Java-/VB-Scripts and Java Applets are supposed to enrich the Internet experience for users. Personal firewall in mobile phone should give total control over which sites that can activate such a behavior, and which sites that should be stopped. This function could be very useful in preventing pornography. Parents could ban URL addresses, words in the URL address or content on site to be sure that their children would not be an offer of pornography.
Time Control and Account Manager	This function could be useful in mobile phone to check time used for Internet connection. In this way, a user can calculate if the time (minutes/hours) used on the Internet is correct with time calculated in this function. This is a good opportunity for user to check if anyone used Internet connection on users account.

Trusted IPs – mobile phone numbers	Trusted IPs is a useful function in personal firewall for mobile phone to allow only traffic and services from IPs mobile phone trusts. In addition, servers and the other end in P2P could be also seen in context of trusted IPs. With this function user can add single IP address or range of addresses that user trusts and with which user wants to share services. Optionally, this function could be modified as trusted mobile phone numbers list or list specified in GGSN of trusted sites. Trusted mobile phone numbers should be available in a trusted list and services could be exchanged.
Forwarding	This function could be useful in filtering of traffic. All packets with the destination IP matching personal firewall in mobile phone, will go to the INPUT stage. All packets coming to personal firewall but with another destination address then the personal firewall itself will go to the FORWARD stage (described in Chapter 6).
JavaScript Pop-Up blocker	This function is probably one of the most important for personal firewall in mobile phone when using Internet Explorer. With the personal firewall the user is able to block or accept pop-ups that are launched using JavaScript techniques. Downloading java applications goes through personal firewall, which further filters java scripts. Java scripts could contain virus that block some of the operations in the mobile phone, add or remove some of the functions or bomb mobile phone with pop-ups. The pop-up java script is handled by the browser, e.g., Opera can be configured to ignore this, but Internet Explorer cannot. That is why this feature could be important in mobile phone.
Collection of behavioral patterns "Cookies"	A cookie is a small inactive file containing a code that is sent to the browser by web server and stored on the mobile phone. Cookies do not contain personal details as e.g., password, mobile number or address details in text form, so data is safe from abuse. Cookies in personal firewall in mobile phone could be useful in J2ME (Java 2 Platform, Micro Edition) technology to block web pages that could include virus or any other form of errors that could influence mobile phone. Since use of JavaScript in mobile phone has increased in recent years, the need for blocking web pages is essential. JavaScript needs filtering after downloading.
Updating function for a new version	This feature could be useful in mobile phone for updating for new versions of personal firewall. Mobile phone does not allow upgrading or downloading of binary data. This feature could be very useful in mobile phone if it is possible to update new version of software without downloading new software (described in Chapter 6).

3 Possible attacks on mobile phone

First, this chapter describes connection between virus threats and personal firewall, relating to different types of virus. Furthermore, useful functions in personal firewall that possibly could prevent virus related threats will be proposed.

Possible attacks on mobile phone and solutions how to prevent these attacks will also be disccussed. Vulnerability to security attacks from the network regarding different types of attacks will be outlined. Useful functions in personal firewall to prevent described attacks will be proposed. At the end, functionality personal firewall should have will be outlined i.e. what security measure should be taken.

3.1 Virus related threats

While the possibility to download advanced applications offers mobile phone users more freedom of choice, more open download environments raise new security concerns. It becomes no longer possible to verify the behaviour of content on every device model before publishing. Actually, it is just a matter of time when virus will start to bomb and inflect mobile phones.

Most systems offer simple SMS-based delivery of ring tones and logos, and in present time more advanced systems allow operators and service providers to distribute multiple types of digital content from screen savers, polyphonic ringing tones and media clips to Java and Symbian applications [7].

PC viruses have no effect on mobile phones, except when using Windows CE OS. There are more and more mobile phones that build on Windows CE: Qtek 2020 PDA, Nokia 9210i and Nokia D211 Multimode Radio Card. For example, Qtek 2020 offers an easy interface, elegant icons and effective software. There are mobile editions of Excel, Word and Outlook. In this way, user is offered access to key information without having a laptop. Mobile phones built on Windows CE could be inflected by viruses since Windows CE is compatible in mobile phones and run Windows applications. That is why these mobile phones are vulnerable for virus attacks in the same way as PC.

3.1.1 Types of virus

It is important to identify what a computer virus is in order to be able to compare it with possible mobile phone virus. Like its biological equivalent, a computer virus is a program that spreads unwanted and unexpected actions through the insides of the PC. Not all viruses are malicious, but many are written to damage particular types of files, applications or operating systems [8].

There are three main types of viruses in circulation: *boot sector viruses*, *macro viruses*, and *file infecting viruses* [9].

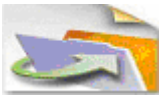
The *boot sector* is the very first sector on a floppy or hard disk. It contains executable code, which helps to operate the PC. Because the PC's hard disk boot sector is referred to every time the PC powers or "boots" up, and is rewritten whenever configuring or formatting the set-up of the system, it is a vulnerable place for viruses to attack.

Macro viruses are by far the most common viruses in circulation. These can be obtained through disks, a network, the Internet, or an e-mail attachment. Macro viruses do not directly infect programs, but instead, infiltrate the files from applications that use internal macro programming languages, such as Microsoft Excel or Word documents. They are then able to execute commands when the infected file is open, which spreads the virus to other vulnerable documents. In turn, users who share files can also spread the virus to other systems. Windows CE mobile phones are vulnerable to this type of virus in the same way as PC since they have open OS. This type of virus may also be a threat for Symbian mobile phones since they also have open application OS.

File infecting viruses infect executable files, such as EXE and COM files, loading into memory when executed and spreading their payload [9]. Probably the most interesting effects of the virus on mobile phones would be caused by this third type of virus, in addition to worms and Trojan horses.

Types of viruses change rapidly through the last years. From virus used to spread within the corporate network to hybrid worms or blended threats. Viruses are becoming more complex and difficult to handle. Mobile phone virus situation is not critical today, but the future is insecure. Since the use of Internet is growing fast in the mobile phones, changes in virus behavior will probably also influence mobile phones [8].

Table 3.1 Changes in virus behavior



Mid-1990s: Viruses started using network shares to spread within the corporate network. Pure worms that spread by using network shares or e-mail did not exist at the time.

Late 1990s: Virus writers had begun using e-mail as a means of spreading viruses; the e-mail worm was born.

Early 2000s: Writers of malicious code began expanding the capabilities of viruses and worms, creating the first hybrid worms.

Today: Hybrid worms, or blended threats, use multiple mechanisms to spread, combining traditional hacker techniques to find operating system or software vulnerabilities with virus-like behavior to spread further and cause damage.

Even if PC viruses have no effect on mobile phones, unless using Windows CE, the principle of attacking would be the same. It is reasonable to assume that mobile phone is not immune.

3.1.2 Other security breaching programs

Strictly speaking, Trojans[2] and worms[3] are not viruses by definition. Trojans could be programmed to copy for example mobile phone's address book and send it to website. A wireless worm could also be troublesome for mobile phone users. It could e.g., send content from web pages (page could include insecure content) to everyone in user's address book, while browsing on the Internet.

E-mail is a good opportunity to spread viruses. Often the increasing desire for integration between e-mail programs and office applications has left security holes that are quickly exploited by worms such as ILOVEYOU[4] [9]. This was the case of PC virus, but mobile phone using Windows CE could also be victim to this kind of virus. This is relevant for mobile phone since the use of e-mail via mobile phones is constantly growing.

3.1.3 Can personal firewall protect against viruses?

Some of the functions in personal firewall, proposed in Chapter 2.6, could be useful in preventing mobile phone from being inflected by malicious software such as: virus, Trojan and worms. These functions are: monitor incoming and outgoing traffic, detection intrusion attempts and active content nuisance.

Monitor incoming traffic should block programs and packets that may include insecure and unusual content. It is up to personal firewall to detect any strange behavior from programs or unusual content in packets. If personal firewall detects this, it should send user a warring. It should also allow only certain trusted servers, applications and IPs to send traffic to the mobile phone user.

Monitor outgoing traffic function in personal firewall should allow only outgoing traffic from trusted list application. This feature is most important regarding Trojans. User should be aware if mobile phone starts to send traffic without his request. Once again, personal firewall should send warning asking user if he/she really wants to broadcast.

Detection intrusion attempts scans for patterns of network traffic that may indicate known attacks intrusion detection. It should include an updatable list of virus detection signatures. This list should be updated each time new virus, Trojan or worm appears.

Active Content nuisance function should give control over which sites should be stopped. If there are sites that are known to include insecure content or malicious software, they should be blocked by personal firewall.

---

[2] Software entity that appears to do something normal but which, in fact, contains a trapdoor or attack program

[3] Standalone program that, when run, copies itself from one host to another, and then runs itself on each newly infected host

[4] E-mail can be structured so just viewing the message is enough to cause infection on a system where the security patches are out of date

Described functions in personal firewall could prevent mobile phone being inflected by malicious software, but at what degree? Malicious software is getting smarter and there are too many ways of encoding binary files for transfer over networks, too many different architectures and viruses to try to search for them all. In general, personal 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. Personal firewall is never a substitute for sensible software that recognizes the nature of what handling-untrusted data from an unauthenticated party, and behaves appropriately.

Figure 3.1 New viruses can bypass gateway-level web and e-mail virus protection

An integrated personal firewall with AV is supposed to give the best protection against malicious software such as viruses, Trojans and worms. AV protection is out of the scope of this master thesis and will be presented only briefly. It is still worth mentioning that personal firewall is alone not enough to protect from malicious software.

3.1.4 How antivirus programs work

The rise in popularity of e-mail worms has increased the need for everyone to have personal firewall and/or AV product protecting their system.

Antivirus (AV) is a term applied to either a single program or a collection of programs that serve to protect PC or mobile phone from viruses. The main component of an AV solution is the scanning engine. The intricate details of each engine vary, but all share the basic responsibility of identifying virus-laden files using virus signature files: a unique string of bytes that identifies the virus like a fingerprint. They view patterns in the data and compare them to traits of known viruses captured in the wild to determine if a file is infected. In most cases they are able to strip the infection from files, leaving them undamaged. When repairs are not possible, AV programs will quarantine the file to prevent accidental infection, or they can be set up to delete the file immediately [9].

Viruses are getting smarter and sometimes it is really hard to define virus signature file. Another scanning method could be to flag suspicious data structures or strange behavior that could indicate virus event. If AV detects any unusual behavior, it quarantines the questionable program and broadcasts a warning about what the program may be trying to do (e.g., modify Windows Registry). Then it is up to user to decide whether to allow or deny this program. This means that AV can be used in corporation with personal firewall that includes Detection intrusion attempt function. In turn, this function has an updatable list of virus detection signatures used to respond to known discovered methods. This proves that an integrated personal firewall with AV is best suitable to protect against malicious software.

3.2 Virus attacks on mobile phones

There have been some minor virus attacks on mobile phones. One of them made it impossible for users to receive any calls, one even made the mobile phone crash. These viruses were easy to fix by a normal phone update. These days the chance of getting mobile phone virus is growing, since it is possible to have bigger data traffic like MMS, GPRS and UMTS (downloading large applications, always-on connection and examples mentioned above).

First warning appeared on the Internet in 1999, when it cautioned mobile phone users to beware of answering calls from "UNAVAILABLE". This virus could erase all IMEI and IMSI information from both phone and SIM card, which will make phone unable to connect with the telephone network [10].

In June 2000, an instance of a computer virus that affected mobile phones was recorded, although this was not a case of a malevolent program inserted into the phones themselves; the cells were merely the final destination of the leg-pull. The *Timofonica*[5] virus was designed to send prank messages to mobile phones on the Telefonica cellular network, which operates in Spain. In addition, the worm sends a message to a so-called short messaging service (SMS) gateway that sends a text message to phone users. The worm randomly generates phone numbers targeting the "corio.movistar.net" SMS gate. Every time the worm is forwarded to a new address, it sends a new SMS message to a randomly selected number, thus bombing people with SMS messages [10].

Timofonica did not harm mobile phones any more than a wrong number call damages any phone. However, as wireless technology grows more sophisticated, so does the risk that one of these days there will really be a real virus launched against mobile phones, one that will force its way into units and do nasty little things to them once it is in there.

In 2002, yet another attack on mobile phone was made. Mobile phone users received a phone call and mobiles phone displays "ACE-?" on the screen. Users were recommended not to answer this call and end this call immediately. Those who answered this call got their mobile phone infected by this virus. This virus will erase all IMEI and IMSI information from both mobile phone and SIM card, which will make mobile phone unable to connect with the telephone network, and make mobile phone useless. Over 3 million mobile phones were infected by this virus in USA [11].

[5] This virus was received as an e-mail attachment. When this attachment was open, the virus was sent to every e-mail address in the address book. The worm sends itself to all addresses that are stored in a victim's address book.

3.2.1 Solutions to prevent virus attacks on mobile phone

The two biggest phone software giants Nokia and Ericsson have decided to cooperate in making AV software. These days some secure software can already be found built in mobile phones, mostly in Sony Ericsson phones. This secure software already secures web browsing via mobile phone.

In November 2003, Nokia announced the integration of the *Sophos*[6] virus detection engine on Nokia Message Protector. In the past, enterprises deployed standalone products for their various messaging security needs, e.g., spam prevention, content inspection and virus protection. Now, enterprises recognize that standalone products not only increase administrative burden, they are also expensive, require manual upgrades and often run on insecure platforms. Nokia Message Protector delivers a comprehensive, streamlined and integrated secure content management solution. [12].

With e-mail being one of the most prolific methods for spreading viruses, many organizations have experienced the repercussions of not having extra layers of security against malicious code. With the addition of *Sophos's* unique virus detection engine to Nokia Message Protector, users will benefit from the highest possible level of protection against viruses.

The *Sophos* AV technology provides Internet gateway security to perform each of the following, all on a single, multi-threaded virus detection engine [12]:

- detect all virus types
- detect and disinfect macro, boot sector, and PE executable viruses
- detect viruses in compressed attachments
- detect viruses inside MIME-encoded messages
- detect viruses that “morph” during propagation.

It is important to mention that secure software will automatically install and provide updates for new releases using some kind of automated network service. This ensures that the latest e-mail security technology is deployed across e-mail networks with minimal latency.

[6] Multi-layer security solution purpose-built to protect e-mail against common threats such as malicious software and attacks

3.3 Vulnerability to security attacks from the network

Network security goes hand in hand with mobile phone security, and these days it is really hard to separate the two since mobile phone is capable of having an always-on connection to Internet. Everything from electronic hotel door locks to cellular phones to laptop is attached to networks. As difficult as it is to build a secure mobile phone; it is much more difficult to build a mobile phone that is secure when attached to a network. Network attached mobile phones are pregnable; instead of an attacker needing to be in front of the mobile he is attacking, he can be everywhere across the planet and attack the mobile phone using the network [13].

It is pretty much impossible to talk about mobile phone security without taking into consideration network security. Lots of different types of network could be discussed, but the most interesting is IP (Internet Protocol), i.e. an always-on connection available in mobile phones becomes an interesting target for attackers. Networking protocols seem to be converging on the Internet that is why it makes the most sense to discuss the Internet. Wireless subscribers' always-on connections are vulnerable to attacks internally and externally. This part of master thesis shall be seen in a context of what already exist in IP security functions in the whole chain; from mobile phone to service provider.

3.3.1 Security threats in the mobile environment

Being based on the concept of transferring data through intermediate nodes, the very nature of Transmission Control Protocol/Internet Protocol (TCP/IP), the basic communication protocol over the Internet and Intranets, makes it possible for an adversary to interfere with communications. Any TCP (UDP/ICMP)/IP session may be interfered with in the following ways [14]:

Eavesdropping - the information privacy is compromised without altering the information itself. Eavesdropping may imply that someone has recorded or intercepted sensitive information (e.g. credit card numbers, confidential business negotiations).
Tampering – the information is altered or replaced and then sent on to the recipient (e.g. change of an order or commercial contract transmitted).

Impersonation – the information is passed from or to a person pretending to be someone else (this is also called *spoofing,* e.g. using a false email address or web site), or a person who misrepresents himself (e.g. a site pretends to be a bookstore, while it really just collects payment without providing the good).

3rd generation cellular technology is constantly evolving, supporting broadband, packet-based transmission data, and providing always-on connectivity to mobile phones and other wireless communications. Therefore, all the security threats familiar with in the Internet, invade the cellular wireless networks as well, and translate into risks for commercial transactions, corporate data and personal information.

3.3.2 Types of attacks and the role of personal firewall

There are two types of attacks: active and passive attacks. In passive attacks, the attacker is outside the system and listens in, hoping security lapses will occur. Examples of passive attacks are: sniffing password, network traffic and sensitive information. Probably, the most interesting type of attack taking this assignment into account is active attacks e.g., Man in the middle attack, Denial of Service, breaking into a site and address-IP spoofing (pretending to be someone else).

Man in the middle attack

- Attacker acts as a proxy between the web server and the client
- Attacker has to compromise the router or a node through which relevant traffic flows

Unfortunately, there is not much personal firewall can do to prevent Man in the middle attacks. None of useful functions described in Chapter 2, can protect mobile phone being attacked by Man in the middle (e.g., there are no functions that discover an attacker acting as a proxy between the web server and the user). Instead, one should use authentication (Diffie-Helman [15]), encryption or key agreement (eventually IPSec [16]) as protection from Man in the middle attacks.

Denial of Service

Attacks through with a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it. This can be done by [17]:

1. Crashing the system
2. Exhausting the resources by flooding the system or network with information

There are features in personal firewall that can be use to prevent DoS attacks. Functions like monitor incoming traffic, filtering and blocking in personal firewall can prevent overloading of the system by e.g., dropping incoming packets with the same content (same IP header in several packets) or totally block incoming packets to the mobile phone after receiving many packets in short period. In this way one can protect that memory in mobile phone does not become overloaded. Packet filtering function should prevent buffer overruns, since memory in mobile phone must not be overloaded. Personal firewall can e.g., block all incoming packets after the half buffer size of the mobile phone is used (primary memory in mobile phones is much smaller then for PCs). Another alternative could be filtering function in personal firewall that check incoming IP packets or filter/block packets coming from unknown source.

Personal firewall should allow only certain trusted servers (site) to send traffic to mobile user, otherwise block packets that may content insecure content (described useful function in personal firewall in Chapter 2).

Yet another useful function in personal firewall is Trusted IPs (trusted mobile phone numbers, as described in Chapter 2). This function will only allow incoming packets from trusted IPs (list of contacts) and deny unknown IPs to send packets.

Address IP spoofing

IP packets have source and destination information, but an attacker can modify them. An attacker can create packets that seem to come from one site, but do they really?

To prevent address IP spoofing, personal firewall functions like trust site and trusted IPs (mobile phone numbers) are essential. Personal firewall should allow only trusted sites and mobile phone numbers to send traffic to the mobile users. Otherwise, personal firewall should block traffic and eventually ask if the user wants following traffic (from source IP address) to allow to the mobile phone.

Yet another useful function in personal firewall is monitor outgoing traffic. Monitor outgoing traffic should be based on a checksum of the entire application, instead of name, to prevent renaming of applications. This is discussed in more detail in Chapter 6.

In addition to mentioned solutions, there is not much a personal firewall can do to protect mobile phone from address IP spoofing. How could personal firewall know if the packet information is being modified?

Port Scanning

Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a LAN or connected to Internet via a modem run many services that listen at well-known and not so well known ports. By port scanning the attacker finds which ports are available (e.g., being listened to by a service). Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness [18].

Port scanning usually means scanning for TCP ports, which are connection-oriented and therefore give good feedback to the attacker. UDP, or connection-less traffic, responds in a different manner. In order to find UDP ports, the attacker generally sends empty UDP datagrams at the port. If the port is listening, the service will send back an error message or ignore the incoming datagram. If the port is closed, then the operating system sends back an "ICMP Port Unreachable" message.

One problem, from the perspective of the attacker, with port scanning is that it is easily logged by the services listening at the ports. They see an incoming connection, but no data, so they log an error [18].

There are a number of stealth scan techniques to avoid port scanning error logs. One is the half-open scan that only partially opens a connection, but stops halfway through. This

is also known as a SYN scan because it only sends the SYN packet. This stops the service from ever being notified of the incoming connection.

A more creative approach to port scanning takes advantage of the bounce attack vulnerability in FTP servers, which allows somebody to request that the FTP server open a connection to a third party on a particular port. This allows the hacker to force the FTP server to do the port scan and send back the results.

Port Scanning is obviously very vulnerable to attacks. From the reasons mentioned above, it is necessary to implement functions in personal firewall to prevent such attacks. Probably, one of the most important functions would be port scanning detection and logging. These events occur when a number of packets arrive at the system to different ports from the same source. When this pattern occurs within an interval of time, personal firewall will log this event as port scan. In this way, personal firewall can detect what services the system is providing and could investigate hacking attempts on the system. One major drawback is that it costs to send packets, which are blocked in return, for mobile phone user.

To prevent port scan attacks, port scan function in personal firewall should not answer to empty UDP datagrams and should not send back error message (should not answer to ICMP messages because of the ICMP tunneling [19]). For TCP connection, server should send message (warning) to user when server starts port scanning and inform what kind of service is involved. Rules in personal firewall for which services are allowed to be used (e.g., for P2P only SIP connections) could be implemented to prevent attacks.

Personal firewall should have trusted IPs mobile phone numbers as well. In this way, personal firewall could prevent attacks from unknown IP addresses. Mobile phone should listen only to those services, which are on trusted IP addresses.

3.4 Functionality personal firewall should have

In addition to useful functions in mobile phone regarding personal firewall, AV protection is important related to functionality personal firewall should include, but is out of the scope of this thesis. Since there is an important relation between personal firewall and AV protection, personal firewall should have secure software build in phones. It should also provide functionality for anti virus detection, especially e-mail anti virus detection.

As mentioned previously, monitor incoming (outgoing) traffic, filtering and blocking traffic are some of the most useful functions in a mobile phone, in context of personal firewall. To prevent file inflecting viruses or Trojans, mobile phone should include monitor outgoing traffic function in personal firewall. Every time mobile phone starts to send traffic, user should get warning on the display. When this function is included (enabled), user is aware of what program or content mobile phone is trying to broadcast. In addition to mentioned functions, personal firewall should include Detection Intrusion attempts and Active contents nuisance. This will make user more secure when connected to Internet.

In order to protect mobile phone from being victim to described attacks in Chapter 3.3.2, personal firewall should include proposed useful function in personal firewall. Personal firewall should include functionality to support most important functions: monitor incoming traffic with filtering, trusted servers (sites) and IPs and port scan, regarding described attacks.

In short, to prevent mobile phone from being inflected by malicious software (virus, Trojan and worms) and attacks from the network, personal firewall should have functionality to monitor (filter/block) incoming and outgoing traffic. In addition, personal firewall should have include list of detection intrusion attempts, allow only traffic from trusted sites (servers), applications and IPs and port scanning detection.

4 Analysis of mobile phone functionality

Mobile phones are becoming an attractive target for attackers. There is no doubt that the need for personal firewall in mobile phone becomes essential, especially during the Internet connectivity and downloading Java application, as already mentioned.

This chapter deals with mobile phone functionality that necessitates personal firewall functions. Mobile phone functions that need support from personal firewall and security issues regarding downloadable applications will be described in this chapter including useful functions in personal firewall.

4.1 Mobile phone functions that need support from personal firewall

Both mobile phone standard functions (e.g., WAP and browsing) and mobile phone specific functions (e.g., charging & billing) need support from personal firewall. Since GRPS and UMTS offer an always-on connection and IP connectivity, need for personal firewall becomes essential. Probably, the crucial need for personal firewall would be in downloading Java applications from the Internet, since many Java applications could include insecure content.

There are also Peer-to-Peer (P2P) services over IP in mobile phones e.g., Push-To-Talk, Buddy List and Wireless Village that need support from personal firewall. Security in P2P has to be taken into consideration since open server ports in P2P give a great opportunity for hackers to attack mobile phone while using open port services.

4.1.1 Billing and Charging

Billing & Charging (or accounting and charging) are functions in the network that need support from personal firewall. Those functions are similar. First of all, it is important to define them, in order to distinguish different roles they do:

- *Billing*: write a bill to the subscriber
- *Charging*: collect information of the subscriber behaviour to be able to write a bill.

Billing alternatives are based on: monthly fee (basic and flat-MMS), volume fee (which is the most interesting regarding personal firewall for mobile phone; amount of money for data volume –WAP, and per packet) and time fee [20].

The GPRS specifications stipulate the minimum charging information that must be collected in the stage of service description. These include destination and source addresses, usage of radio interface, usage of external Packet Data Networks, usage of the

packet data protocol addresses, usage of general GPRS resources and location of Mobile Station. GPRS network needs to be able to count packets to charge customers for the volume of packets they send and receive.

Useful functions in personal firewall to support Billing and Charging

Personal firewall should have functions that prevent unnecessary traffic to be a part of bill and watch over charging. Functions in personal firewall that are necessary to support billing and charging are: monitor incoming traffic (filtering and blocking), port scan detection and logging and time control and account manager.

Function monitor incoming traffic is supposed to allow only networks received in response to request user sent out to the Internet to could write a correct bill. It should allow packets for which user configured rules at personal firewall apply. Packets arriving from unknown source should be blocked.

Port scan detecting is useful to distinguish between packets send on users request and packets send from an attacker. This function is also very important for collecting information of the subscriber's behaviour to be able to write a bill. However, there is a problem personal firewall is not able to deal with. Namely, it costs to send blocked packets in return for volume fee. This function should prevent user being charged for blocked packets as a result of port scanning. Port scan detecting can make sure that mobile phone does not send or receive unwanted traffic. Personal firewall shall not answer to ICMP echo-request or empty UDP datagrams, as already mentioned for port scanning. In addition, this function should provide that users do not receive and send unwanted traffic that could increase user's bill. Port scan should not answer and further send outgoing traffic, which could be result of e.g., Trojan.

There is an alternative to this function in the case personal firewall is implemented in GGSN (implementation described in Chapter 6.1.2). Personal firewall has already netfilter in GGSN, which assures that unwanted traffic will not be sent to the mobile phone user. In other words, the user is not being charged for unwanted traffic.

Time control and account manager is a function that personal firewall for mobile phone must include to check time used for Internet connectivity. Probably the best way to check Internet connectivity would be usage of packet data protocol addresses. Time control is also an essential function if using time fee billing alternative, since user is supposed to pay certain amount of money for time used GPRS services. On other hand, account manager is important for volume fee billing alternative, to collect data volume or fee per packet.

4.1.2 Push-To-Talk (walkie-talkie)

Push-To-Talk (PTT) is a two-way communication service that works like a "walkie talkie". A normal mobile phone call is full duplex, meaning both parties can hear each other at the same time. PTT is half-duplex, meaning communication can only travel in one direction at any given moment. To control which person can speak and be heard, PTT requires the person speaking to press a button while talking and then release it when they are done. The listener then presses their button to respond. This way the system knows which direction the signal should be traveling in [21].

PTT systems were introduced in 2002 that use VoIP (voice over IP) technology to provide PTT service digitally over 2.5 and 3G data networks. Network uses packet switching to route calls, i.e. voice data from the caller is chopped up into packets, sent, and then reassembled at the recipient's end. This is efficient because only relevant data i.e. speech is transmitted. Rather then being a replacement of long, interactive communication, PTT is best suited for demands for quick communication among end-users.

Technology Supporting Push to Talk

At the core of PTT is an IETF standardized protocol known as Session Initiation Protocol (SIP) used for IP communications and Wireless Softswitch network infrastructure. Being that it uses IP as a transport/bearer, PTT is highly dependent on the rollout, expansion and improvements of 2.5G and 3G technology and infrastructure [22].

Multimedia Integration with PTT

Integration of MMS and other advanced messaging features with PTT service makes sense because both services are a VAS, but perhaps more so, because of the service synergy opportunities. For example, a user could (1) detect a friend (Presence), (2) find a friend (LBS – Location-based Service), (3) talk to a friend (PTT) and/or message with a friend (MIM), and then (4) send multimedia messages (MMS) or engage in other Advanced Messaging Services with a friend.

Person-to-person communication, like Presence, Instant Messaging, VoIP and video applications offer clear benefits for enterprise and money savers. SIP is simple protocol and Internet standard based which in turn gives clear advantages over older protocols.

Useful functions in personal firewall to support PTT

Developing SIP protocol raises new security issues. Probably the most interesting is how to keep communication ports open only for the time to let communication pass. All the other times the ports should remain closed. The only long-term viable solution is where personal firewall is made aware of SIP signaling and where the personal firewall itself allows ports to be opened for just long enough to allow communication to pass and then

be closed again. This is by definition the most secure system, as ports stay open for the minimum amount of time possible [23].

Because of the open nature of the SIP protocol, the systems involved have to provide functionality for authenticating users at registration. Next security issue is that heavy data usage affects the quality, especially of voice communication. The solution might be that personal firewall functionality has the ability to limit bandwidth and set priority for different types of traffic. Ideally, personal firewall should distinguish between SIP based and other traffic; therefore being able to give priority to the SIP based person-to-person traffic.

There are also other security risks with SIP as e.g., DoS prevention, register protection, end-to-end authentication and end-to-end message confidentiality.
Reasons discussed above lead to one solution: implement personal firewall.

Using a SIP over IP means setting up two separate connections, which are related:

1. connection for signaling message
2. connection for signaling media

Registration to SIP proxy server goes over TCP or UDP (optional), while media transmission goes over UDP. Both connections need protection from the personal firewall. Personal firewall should include following functionality: block/filter unexpected media packets in outgoing calls, block/filter incoming unexpected signaling packets, block packets carrying invalid protocols, and port scan detection and trusted IPs (allow communication with only trusted IPs or phone numbers), which were already discussed.

By blocking the packets that carry invalid protocol or came from unknown (unauthorized) sources, denial of service attacks could be prevented. This is why blocking incoming and outgoing traffic is an important functionality personal firewall should include.

There are also some other security concerns that personal firewall cannot do much to prevent (e.g., message encryption and confidentiality). Possibility to encrypt messages before passing over the Internet is handled by SIP standard, which contains a part on such encryption, passing SIP over TLS.

By trusted IPs functionality is meant that personal firewall allows only persons from trusted list of contacts to start the communication to other end or ask the user if he/she wants to communicate (add to list of contacts) following phone number. There must be functionality in personal firewall unit that serves as the SIP register for user authentication.

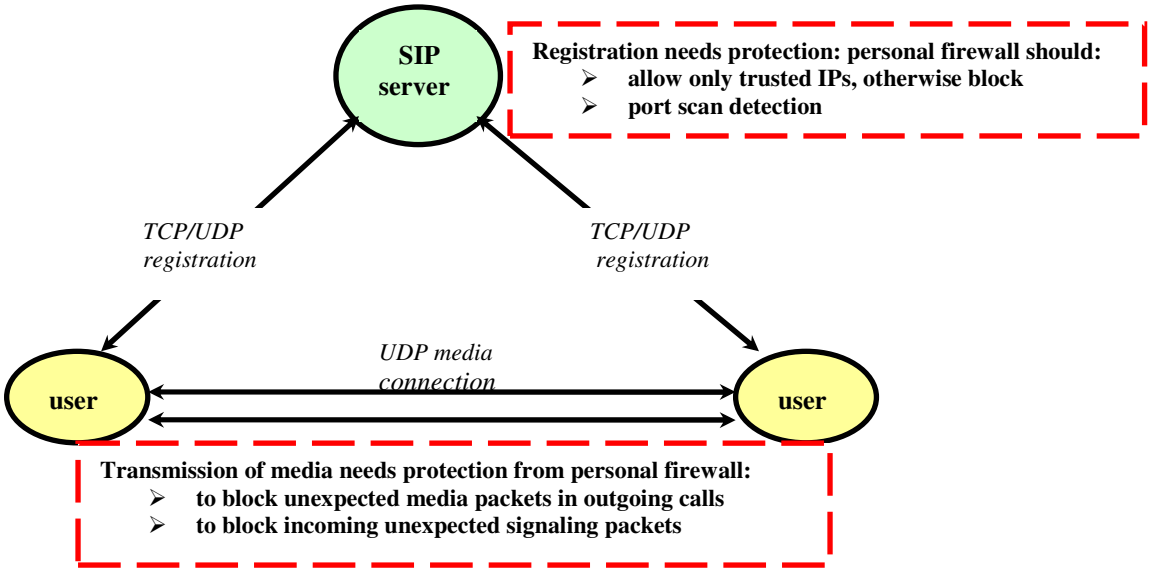


Figure 4.1 Peer-to-Peer communication over SIP

4.1.3 Buddy list (find friends)

Buddy list function in mobile phone is half-standardized function variant that offers P2P service. At the core of Buddy list is SIP protocol over IP. Buddy list in mobile phone could be compared to MSN chat on PC. It shows a list of friends online at the moment and available friends for chat. From the buddy list, user can choose a friend from e.g., address book, to chat with.

Useful functions in personal firewall to support Buddy list

Just like PTT needs support from personal firewall, Buddy list needs the same support since at the core of this mobile phone function is SIP over IP. Personal firewall in mobile phone should therefore include the same functionality for Buddy list as for PTT.

4.1.4 Wireless Village

The Wireless Village (WV) initiative is about building community around new and innovative Mobile Instant Messaging and Presence Services (mobile IMPS). Instant Messaging and Presence is moving from the desktop and Internet to the mobile domain. Ericsson, Motorola and Nokia recognize the need for an industry standard for mobile IMPS. These companies formed the WV Initiative to ensure the interoperability of wireless messaging services and IM in particular [24].

Figure 4.2 Wireless Village

The WV IMPS includes four primary features: Presence, Instant Messaging, Groups and Shared Content.

In the Wireless Village model, *Presence* takes on a richer meaning. It includes client device availability (phone is on/off, in a call), user status (available, unavailable, in a meeting), location, client device capabilities (voice, text, GPRS, multimedia) and searchable personal statuses such as mood (happy, angry) and hobbies (football, fishing, computing, dancing). Since presence information is personal, it is only made available according to the user's wishes – access control features put the control of the user presence information in the users' hands.
Instant Messaging is a familiar concept in both the mobile and desktop worlds. Desktop IM clients, two-way SMS and two-way paging are all forms of Instant Messaging. WV will enable interoperable mobile IM in concert with other innovative features to provide an enhanced user experience.

Groups or chat are a fun and familiar concept on the Internet. The WV initiative enables both operators and end-users to create and manage groups. Users can invite their friends and family to chat in-group discussions. Operators can build common interest groups where end-users can meet each other online.

Shared Content allows users and operators to setup their own storage area where they can post pictures, music and other multimedia content while enabling the sharing with other individuals and groups in an IM or chat session.

The WV specification uses the security mechanisms of underlying transports and IP. Thus no new security scheme has been defined. Authentication between a WV IMPS client and server assures that the client and server are who they say they are. In addition, instant messaging traffic can be encrypted to allow for secure instant messaging.

Useful functions in personal firewall to support Wireless Village

Even thought, WV is innovative and offers new features in mobile phones, WV has one weakness: vulnerability to both passive and active attacks. Since WV is a P2P service (open ports) over IP, support and protection from personal firewall is essential.

Port scan detection and logging is the function in personal firewall that needs to support this technology, just like other P2P services over IP (PTT and Buddy list). Already discussed, P2P communication is very vulnerable to attacks. Personal firewall is supposed to log events (arriving the packets at the system to different ports but from the same host), as a port scan. The purpose of port scans is to discover services the system is providing and could be investigated. Furthermore, mobile phone could be protected e.g., by not answering on ICMP echo-request or not answer on TCP port that server does not listen to.

4.1.5 WAP/WWW

WAP and WWW allow the introduction of hypertext services to mobile systems. The services are stored on servers in the network, and they are used with a browser program from the mobile terminal. Both the operator's network and the service provider's WAP servers can be connected to the public Internet, thus exposing the WAP stack and servers to attacks. Some threats to the WAP protocol stack are shown in figure 4.3 [25].

Both WAP and WWW need support from the personal firewall. Introducing an always-on Internet connection to mobile systems made mobile phones vulnerable to attacks. This is the main reason why these mobile phone functions need protection from the personal firewall.

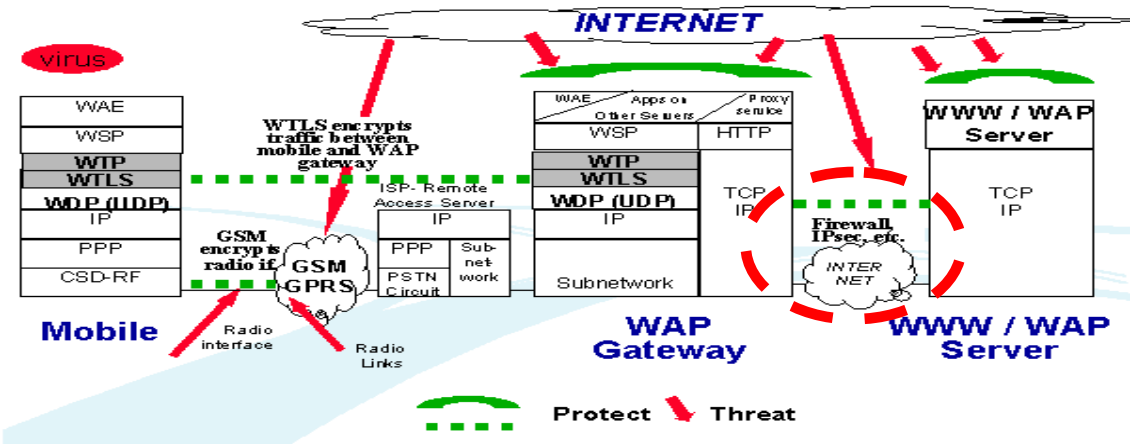


Figure 4.3 WAP architecture and threats

Useful functions in personal firewall to support WAP and WWW

Monitor incoming traffic, filtering and blocking is a function personal firewall should include monitoring packets coming from Internet. One solution would be to allow only certain servers to send traffic to the mobile user. Another solution would be to allow all servers to send traffic to the mobile user, but in this case personal firewall is supposed to detect a likely attack and react by filtering or blocking such traffic.

Detection intrusion attempts can scan for patterns of network traffic that indicate a known attack intrusion attempt. Personal firewall should have an updatable list of intrusion-detection signatures to newly discovered attacks methods.

Trust site function will warn sites that may include insecure content, e.g., virus. Personal firewall would send a warning message to the mobile phone user and ask if he/she really wants to connect to the given site.

Active content nuisance is very important function in personal firewall while using WWW. It gives total control over which sites that can activate, and which should be banned. Personal firewall can include list of the ban URL addresses or words in the URL address to protect children and youth being offers of pornography.

JavaScript Pop-Up blocker is very useful function in personal firewall while using WWW, especially Internet Explorer. As earlier mentioned, mobile phones java libraries for mobile phones are much smaller then for PC, to be able to fit into mobile phone's memory. Once there is a networking (TCP/IP) functionality, it is possible to write a WEB browser for the mobile phone. The browser will connect to a web site, download the page, and will work hard to make the contents visible. Support for images (e.g., gif) has to be handled by the browser as well. The browser will tell the web server, what kind of information it can handle. JavaScript and ActiveX are also handled by browser. If the browser does handle JavaScript, it does tell the web server. Then the web server can send pages including JavaScript. In other words, the web server will send different pages to different browsers. In general, popup via JavaScript is handled by the browser. Internet Explorer needs support from personal firewall, which is the main reason why pop-up blocker is essential. JavaScript could contain insecure content that needs to be filtered or blocked by pop-up blocker. JavaScript Pop-Ups blocker is very useful function in preventing events such as: bomb with pop-ups, blocking, deleting files, sending e-mail, and read personal financial and credit cards.

"Cookies" is very useful function in personal firewall. It can collect and use provided information about browsing habits, such as "referrer". In this way, web pages that contain insecure content can be blocked to prevent inflection of viruses. This function gives the user opportunity to block or accept pop-ups that are launched using JavaScript. Personal firewall checks applications that contain JavaScript to prevent mobile phone from being inflected by possible virus.

4.2 Security issues regarding downloadable applications

The leading mobile phone manufacturers see mobile services enter a new era due to a combination of new capabilities and functionality in mobile phones and networks. A new generation of user experience is enabled by these capabilities which include color displays, more memory in phones, graphical user interfaces, a new generation of browsers (XHTML browsers with a TCP/IP communications stack), packet radio (GPRS), multimedia messaging (MMS) and downloadable applications (Java midlets or Symbian applications) [26].

As a consequence of the new era of mobile functionality, all service providers should revisit their mobile strategies and take into account new opportunities in offering mobile services to their customers such as e.g. mobile ticketing, allowing for a combination of remote purchase and downloading of electronic tickets to the mobile phone. This new era of mobile functionality implies also security issues to be taken into consideration, especially while downloading Java application from the Internet and during Internet connectivity (e.g., sending IP packets).

4.2.1 J2ME (MIDP)

The Java2 Platform, Micro Edition (J2ME) is the Java platform for consumer and embedded devices such as mobile phones, PDAs, TV set-top boxes, in-vehicle telematics systems, and a broad range of embedded devices. J2ME platform is a set of standard Java APIs defined through the Java Community Process program. The J2ME platform delivers the power and benefits of Java technology tailored for consumer and embedded devices, including a flexible user interface, robust security model, broad range of built-in network protocols, and support for networked and disconnected applications. With J2ME, applications are written once for a wide range of devices, are downloaded dynamically, and leverage each device's native capabilities [27].

The Mobile Information Device Profile (MIDP) is the Java runtime environment for today's mobile information devices such as phones and entry level PDAs. MIDP defines a platform for dynamically and securely delivering highly graphical, networked applications to mobile information devices [28].

MIDP enables truly networked applications with a great end user experience on mobile information devices. To download a MIDP application, a user browses a list of applications stored on a Web server. Once the application is selected, the device checks the application to make sure it can run it. If it can, the device downloads the application, and then verifies and compiles its Java byte code to run on the device. Once installed, MIDP applications can be easily updated and removed by the end user.

Multimedia and Game Functionality

MIDP is ideal for building portable games and multimedia applications. A low level user interface API complements the high level API, giving developers greater control of graphics and inputs when they need it. A game API adds game-specific functionality, such as sprites and tiled layers that take advantage of native device graphics capabilities.

Extensive Connectivity

MIDP supports leading connectivity standards, including HTTP, HTTPS, datagram, sockets, server sockets, and serial port communication. MIDP also supports SMS and Cell Broadcast Service (CBS) capabilities of GSM and CDMA networks through the Wireless Messaging API (WMA) optional package [28].

Over-the-Air Provisioning

A major benefit of MIDP is its ability to dynamically deploy and update applications over-the air. The MIDP specification defines how MIDP applications are discovered, installed, updated and removed on mobile information devices. MIDP also enables a service provider to identify, which MIDP applications will work on a given device, and obtain status reports from the device following installation, updates or removal.

End-to-End Security

MIDP provides a robust security model, built on open standards, that protects the network, applications and mobile information devices. The use of HTTPS leverages existing standards such as SSL and WTLS to enable the transmission of encrypted data. Security domains protect against unauthorized access of data, applications and other network and device resources by MIDP applications on the device. By default MIDP applications are not trusted, and are assigned to untrusted domains that prevent access to any privileged functionality. To gain privileged access, a MIDP application must be assigned to specific domains that are defined on the mobile device, and are properly signed using the X.509 PKI security standard. In order for a signed MIDP application to be downloaded, installed and granted associated permissions, it must be successfully authenticated [28].

Useful functions in personal firewall to support downloadable applications (J2ME)

Since MIDP supports leading connectivity standards, including HTTP, HTTPS, and datagram, support from the personal firewall becomes more significant. Personal firewall could prevent some of the following examples of strange behavior from mobile phone such as: sending sensitive information from mobile phone, sending e-mail, SMS or MMS to all contacts in phone book, downloaded application starts to send something to the Internet. Probably, the most dangerous would be if downloaded application starts to open server ports. Personal firewall should send user warning or message. All such strange behavior from mobile phone should be stopped or blocked by personal firewall until the

user has accepted if he/she wants to send to the Internet. In this way Trojan horses could be prevented.

Other important functions personal firewall should include are: Active content nuisance, JavaScript Pop-Ups blocker and Collection of behavioral patterns “Cookies”. Problem statements would be the same as for browsing (WAP/WWW) and these functions are important features in personal firewall regarding downloadable applications. Personal firewall should include these functions. One example of protecting mobile phone is that personal firewall warns the user if the user really wants that the downloaded game shall send IP packets.

4.3 Main reasons why personal firewall is essential

The need for personal firewall in mobile phone is essential, as already mentioned many times. Personal firewall should prevent attacks from network, support functions in mobile phone and protect mobile phone during the Internet connectivity and downloading applications from the Internet. The list below summarizes the main reasons why personal firewall is important.

- Prevent attacks from the network such as: address IP spoofing, port scanning and DoS. For example, DoS can cause reducing of quality of service for all users on the network. This could be prevent by implementing following functions in personal firewall: monitor incoming traffic, filtering and blocking, trust site and trusted IPs, monitor outgoing traffic, and port scan and logging, as described in Chapter 3.

- Prevent so called billing attacks in which someone can run up someone else's bill simply by sending them IP traffic.

- Mobile phones are small devices with limited memory and CPU resources, so DoS attack and billing attack could have the additional effect of consuming extra processing power on these small devices and draining their battery. This is the reason why mobile phone needs support from the personal firewall.

- Support mobile phone functions:

    - Mobile phone specific functions: Billing & Charging, P2P services over IP such as: PTT, WV and Buddy list.
    - "Old" functions in mobile phone: WAP, WWW and e-mail.

- Protect mobile phone from being inflected by viruses and insecure content in downloaded games and java applications from the Internet and in the case of web browsing (WWW/WAP). Mobile phones enabled capabilities such as: more memory in phones, graphical user interfaces, a new generation of browsers (browsers with a TCP/IP communication stack), GPRS, MMS and downloadable applications raise new security concerns and will be more vulnerable to attacks compared to first generation of mobile phone. To be able to download applications from the Internet in secure way, mobile phone needs support from personal firewall. This could be done by implementing following functions in personal firewall: Active content nuisance, JavaScript Pop-Ups blocker and Collection of behavioral patterns "Cookies".

- Protect mobile phone during Internet connectivity, since an always-on connection is a target for an attacker.

5 Various connection types

This part of master thesis deals with discussion on various connection types, regarding security issues in GPRS/UMTS, WLAN, Bluetooth, Internet and Intranet. Vulnerability to attacks in these connection types and which personal firewall functions might prevent and protect mobile phone from attacks is discussed in this chapter.

5.1 GPRS and UMTS

GPRS and UMTS are an extension to GSM, which enables packet, switched networking in order to provide better support for non real-time applications and provide the mobile user with fast and easy access to the Internet [29]. By connecting these networks to the Internet, the mobile terminals become easy target to a variety of attacks. If the operator charges per volume, a variety of attacks where huge amount of unwanted data is sent to and from the GPRS or UMTS mobile station, become attractive.

The main advantage of GPRS and UMTS is that the radio resources are exploited more efficiently since a connection is established on demand and maintained where there is data to be sent or received. Comparing to GSM CS data, GPRS and UMTS are vulnerable to a number of attacks since they offer an always-on connection, such as: garbage attacks, overbilling, IP packet/address spoofing, DoS and Man in the middle.

In garbage attack, a user is being flooded with extra traffic to increase the bill. To prevent these attacks, personal firewall should include monitor incoming and outgoing traffic to prevent overbilling. This could be done by blocking/filtering the packets that may include insecure content in personal firewall, and not allowing illegitimate packets through. Also useful function would be to send a warning to the user if an unusual amount of the data is sent to a GPRS (UMTS) user, and ask if he/she wants to accept these packets.

Overbilling in GPRS/UMTS takes advantage of open connections by flooding the network with unwanted traffic (described in Chapter 4.1.1). Personal firewall should prevent mobile users from receiving unsolicited and unwanted data in an attempt to inflate the account charges of an unsuspecting customer. Monitor incoming traffic should allow only packets received in response to request user sent out to the Internet to write a correct bill. Time control and account manager function should be used to check time used for Internet connectivity.

In IP packet/address spoofing, an attacker sends packets to servers on the Internet with a false source IP address. There is no function in personal firewall that could detect failure of the firewall placed between GPRS/UMTS network and Internet. If this firewall fails to detect these attacks, personal firewall in mobile phone might avoid this kind of attack if it only allows only trusted sites and mobile phones to send packets, and block packets with unknown address.

DoS attacks could be introduced to the UMTS/GPRS network from the Internet as a result of introducing various Internet services to the MS user. These attacks aim to block the communication of the host, immediate node or link by flooding it with bogus packets. To prevent such attacks, personal firewall should monitor incoming traffic and block the packets that may contain insecure content, or allow only certain trusted servers to send traffic to the mobile user.

In Man in the middle attacks there is unfortunately nothing a personal firewall can do. There are no functions that might detect an attacker. Instead, mutual entity authentication based on challenge response mechanism is used in UMTS.

Broadcasting of packets on application level as a result of Trojan (described in Chapter 3.1.1) in GPRS/UMTS could be prevented with monitor outgoing traffic function in personal firewall. If mobile phone starts to send e.g., SMS or MMS (it costs to broadcast), content of address book or other sensitive information to other users, personal firewall should monitor outgoing traffic and ask the user if the user wants to send this information to other users.

Multihoming is used to describe a host that is connected to more than one network at the same time, being reachable through more than one IP address. Being multihomed makes a device connected to the network more resistant to network failures and the bandwidth increases if several links can be used simultaneously. Each PDP Context has its own IP address. Multihoming has multiple PDP contexts.

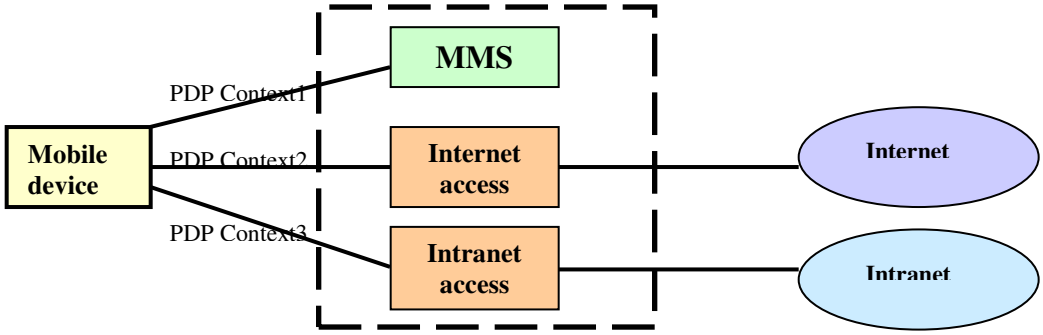


Figure 5.1 Multihoming in GRPS/UMTS

Problem with multihoming in GPRS/UMTS, regarding security issues, is that the information can be forward between different connection types: e.g., forwarding IP packets between Internet and Intranet. Forwarding IP packets from one connection to another may result in inflecting other connections with insecure contents. Personal firewall in mobile phone should include function monitor incoming traffic per PDP context, since the attacker may use several open connections. Another useful function personal firewall should prevent is to set up other connections while using the Intranet.

Personal firewall could be implemented as software in mobile phone, as already mentioned. Another possible solution to prevent attacks on mobile phone could be to implement personal firewall at GGSN in GPRS/UMTS network for a group of users (as

shown in the Figure 5.2). In addition to already mentioned useful functions in personal firewall: monitor incoming traffic, trusted site, blocking/filtering, detection intrusion attempts, etc., personal firewall in GGSN should also protect a group of users while their mobile phones are not active. This solution could be useful to protect a group of users in e.g., companies. Personal firewall could protect mobile phones from being infected by packets that may contain insecure contents while users are not available. It should also prevent e.g., downloading of applications from the Internet while users are unavailable. Personal firewall should send the users a warning and not begin downloading until the user has accepted.

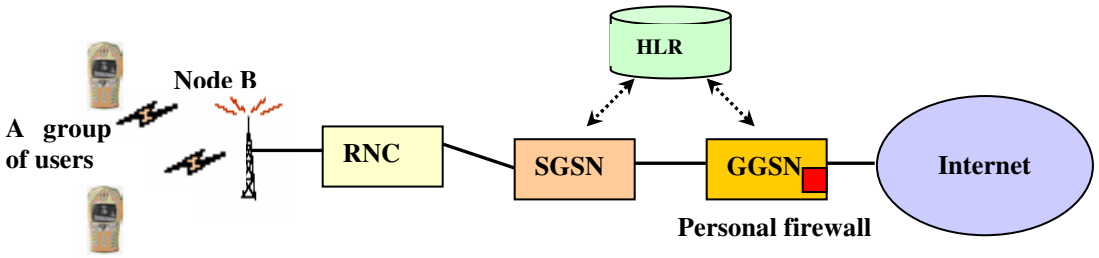


Figure 5.2 Implementing personal firewall at GGSN in GPRS/UMTS

5.2 WLAN

A wireless LAN is the perfect way to improve data connectivity in an existing environment without the expense of installing a structured cabling scheme. Besides the freedom that wireless computing affords users, ease of connection is another benefit. WLAN are here to stay and can only grow in popularity. Because of its popularity and constant growth, WLAN needs to be secure to use.

WLAN is vulnerable to e.g., DoS attacks, Spoofing MAC/IP addresses, Man in the middle attacks and Eavesdropping. The relatively low bit rates of WLANs can easily be overwhelmed and leave them open to DoS attacks or by flooding from fast Ethernet segments [30]. WLAN is more vulnerable to attacks on the link level comparing to GPRS/UMTS.

Once the user is connected to the IP-network, he is open to all threats that he would be while connected to any other means. To perform any type of attacks in the WLAN, the attacker needs access to the network in some way. For certain types of attacks, the attacker does not need to be a part of the network (e.g., DoS attacks).

MAC and IP addresses are sent in the clear text (are not encrypted) the attacker can record these. When the attacker knows the MAC/IP address-pair of a user currently connected, he can set up his own addresses to the same value [30]. There is not much a personal firewall can do to prevent such attacks, but try to prevent masquerading, e.g. prevent another user to use his MAC/IP address pair, and keep on using it after legitimate user left the area, or perform re-authentication at regular intervals.

WLAN is vulnerable to Man in the middle attacks. Once an attacker has successfully become Man in the middle, he could present a fake login-screen to the user, e.g. ask the user to re-authenticate and steel the user's credentials. If volume based charging is applied, an attacker could flood a user with garbage packets, just to increase the user's bill [31]. There is nothing personal firewall can do to prevent such attacks.

To count garbage attacks from the Internet, the WLAN could be protected by personal firewall. There would be need for function in personal firewall that can distinguish legitimate traffic from bogus traffic with high probability. Another useful function would be to configure personal firewall, and allow only IPSec protected traffic.

Open platform terminals may be infected by virus or other malicious software. Trojans may perform all the usual activities, and forward the information to other machines or mobile phones [31]. The real threat is ability to export the credentials for use elsewhere (e.g., sending content from the (U)SIM, and not Trojan's access to credentials itself. Personal firewall has to monitor outgoing traffic and make user aware of forwarding of sensitive or other information. Another function personal firewall should include in this case is Detection intrusion attempts.

Broadcasting of packets in WLAN is a standard Ethernet type broadcasting. It could result in infecting PC with virus. Personal firewall should monitor outgoing traffic to prevent spreading of possible virus from mobile phone to PC or Intranet.

WLAN is susceptible to both attacks on data content and user authentication. These facts allow an attacker to intercept data and gain access to a network by impersonating a valid user. WLAN needs protection both from the attacks from the Internet and inside the range.

5.3 Bluetooth

Bluetooth is a short-range wireless technology that connects various devices and allows restricted types of ad hoc networks to be fashioned. WLAN 802.11b is largely applied to LAN access, while BT LAN access is only one of many applications, most of which focus on smaller Personal Area Networks (PANs) [32]. Like WLAN, BT is vulnerable to attacks on the link level. The typical attacks against BT are eavesdropping, Man in the middle, piconet (service) mapping and DoS attacks.

Eavesdropping allows malicious user to listen to or intercept data intended for another device. BT uses a frequency-hopping spread spectrum to prevent this kind of attack [33]. In BT one-way challenge authentication is used, which is vulnerable to Man in the middle attacks. Unfortunately, personal firewall cannot do much to prevent these attacks. DoS attacks flood the device with requests and deny the user usage of the device. Monitor incoming traffic is a useful function in personal firewall to prevent DoS attacks. Personal firewall should block/filter traffic that may include insecure content, or send a warning to the user regarding accept of these requests.

Broadcasting in BT on link level (master sends message to other slaves) could result in infecting PC via BT link, if the message master forwarded to other slaves has already been infected. Personal firewall should monitor outgoing traffic to prevent spreading of possible viruses from mobile phone to PC or Intranet.

The user must be sure that no one else can access the network using his credentials to perform illegal activities or simply gain "free access" on user's bill. The link between PC and mobile phone must be secured. Infrared can be assumed physically secure, and Bluetooth will depend highly on the current BT security mechanism. If mobile phone starts to send (U)SIM content or other sensitive information to the Internet, as a result of Trojan or other malicious software, personal firewall should have monitor outgoing traffic and ask the user if he wants to send to the Internet.

An example of BT technology can be described in following way; one mobile phone is connected to PC via Bluetooth and connected to both Intranet and Internet. BT Server in mobile phone behaves as a switch between Intranet and Internet. PC is not connected to the Internet, so mobile phone behaves as a switch from PC to Intranet.

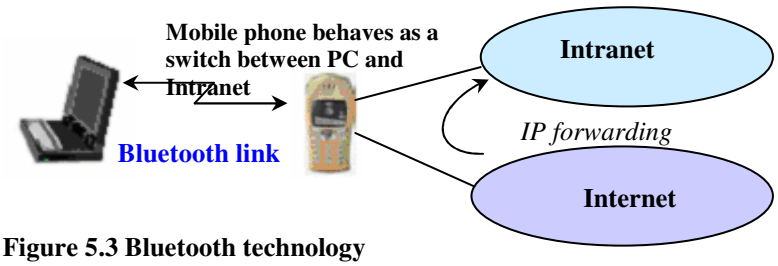


Figure 5.3 Bluetooth technology

This example describes also BT technology usage in multihoming, since mobile phone is connected to Intranet and Internet at the same time. This scenario shows vulnerability if mobile phone starts to forward packets that may contain insecure contents between Internet and Intranet and further damage PC connected to the mobile phone via Bluetooth link. Another threat in this scenario are Trojans, since they may perform certain activities e.g., forward the sensitive information from the mobile phone or machine to the Internet or other mobile phones. Personal firewall should monitor outgoing traffic and send a message to warn the user if he is aware of content in traffic that he wants to send.

Personal firewall in mobile phone should include function that allows only one connection at the time when BT technology is used. In this way inflecting of PC by viruses or Trojans could be prevented. Even if PC is connected to the Internet via mobile phone, there is a chance of stealing personal information from the PC, as already mentioned. Personal firewall shall prevent that such attacks do not occur, by using function such as no IP forwarding between the different interfaces.

Another problem in described BT scenario could occur even if only one connection is set up if mobile phone starts forwarding applications e.g., Java downloads to the Intranet. In this way Intranet could be infected by possible viruses in these applications. In this case personal firewall should ask the user if he/she wants to download these applications to the Intranet, and not start downloading application without user's knowledge.

Figure 5.1Functions in personal firewall for GPRS/UMTS, WLAN and BT

Possible attacks	GPRS/UMTS	WLAN	BLUETOOTH
Garbage attacks ***Overbilling only for GPRS/UMTS***	- Monitor incoming traffic (Block/filter) - Sending a warning to the user - *Time control and account manager*	- Distinguish legitimate from bogus traffic with high probability - Only IPSec traffic goes through	- Monitor incoming traffic - Blocking/filtering - Sending a warning to the user
IP packets/address spoofing	- Trusted sites - Blocking	- Trusted sites - Blocking	¤[7]
DoS	- Monitor incoming traffic - Trusted servers	-Monitor outgoing traffic -Detection intrusion attempts	- Monitor incoming traffic (block/filter) - Trust site
Man in the middle	------[8] This kind of attacks are usual against GGSN in the network (firewall deal with them) and SGSN from other MS's Should use mutual entity authentication	------	------ Should use mutual authentication.
MAC/IP address spoofing	******[9]	- Request logout - Performing re-authentication	¤
Multihoming: (Vulnerable in the case of IP forwarding between different connections)	- Only one connection at the time - Never set up other connections while connected to the Intranet - Monitor outgoing traffic to prevent sending of application on the Intranet.	- Only one connection at the time - Never set up other connections while connected to the Intranet	- Only one connection at the time - Never set up other connections while connected to the Intranet. - Not allow IP forwarding between several connections.
Broadcasting	- Monitor outgoing applications traffic	- Monitor outgoing link traffic	- Monitor outgoing link traffic

[7] Not discussed
[8] Nothing personal firewall can do
[9] Not relevant here

6 Underlying functionality to get a working personal firewall

This chapter includes proposals of what underlying functionality the mobile phone must provide to get a working personal firewall. Discussion on implementation of personal firewall as software in mobile phone vs. personal firewall in GGSN and mobile phone for GPRS/UMTS network with its weaknesses and strengths will be outlined, emphasizing underlying functionality. Protocol stack layer's need for personal firewall and functionality mobile phone has to support will also be discussed.

6.1 Personal firewall in mobile phone vs. GGSN (GPRS/UMTS)

Personal firewall for mobile phone could be implemented in two possible ways: as software in mobile phone or in GGSN and mobile phone for GPRS/UMTS. If personal firewall is implemented in mobile phone, the user sets rules for configuration of personal firewall. In another words, it is configured by user himself. Otherwise, if personal firewall is implemented in GGSN, operators offer services in personal firewall, and user can extend these rules. In other words, a user or a group of users can add wanted services in personal firewall.

One of the main disadvantages in implementing personal firewall in GGSN and mobile phone is that is best suitable for GPRS and UMTS networks. The reason is that GGSN handles incoming traffic from the network and it is best suitable for GPRS/UMTS type of access.

It is less suitable for other connection types because of roaming between e.g., WLAN and GPRS/UMTS. When roaming takes place, personal firewall implemented in GGSN will not be able to protect mobile phone in different type of network (e.g., WLAN). Personal firewall will still reside on GGSN while mobile phone will be connected to WLAN. There is no direct connection between personal firewall in GGSN in GPRS/UMTS and WLAN network. If personal firewall is implemented in mobile phone, it could still protect mobile phone after roaming. Personal firewall in mobile phone as software is suitable for all connection types discussed earlier in Chapter 5, which is a great advantage.

6.1.1 Personal firewall in mobile phone

In order to implement personal firewall, mobile phone has to provide certain functionality to get a working personal firewall. These functionality are e.g., servers and applications which mobile phone trusts, what kind of traffic it will accept, support pop-ups filters, updating for a new version, recognition if the application will start client or server and support application authentication. In short, underlying functionality in mobile phone has to support trusted servers, sites and applications in personal firewall.

Personal firewall in mobile phone has filtering rules, which mobile phone should support. Traffic acceptance is based on e.g., servers (sites), applications and IPs traffic comes from. If traffic originates from an application (server, sites or IP) that personal firewall does not support, these packets will be blocked. If packets are received from applications that did not get permission to send personal firewall will also block them. The same will happen if traffic is sent to applications that are not allowed to send. Personal firewall will not allow traffic from several connections for an application. It could also be configured so that only trusted servers, sites and applications can send traffic to mobile phone.

Mobile phone must support the same applications for which filtering rules exist in personal firewall. It should also have underlying functionality that supports servers it trusts and allow only trusted serves to send to the mobile phone.

Mobile phone must support filtering outgoing traffic, which should be based on checksum of the entire application, instead of application name. Mobile phone should provide method to calculate checksum of the entire application based on e.g., authentication certificate. Each application should be authenticated in personal firewall by a certificate. Personal firewall should include list of certificates and user could add more applications (certificates) he/she wants to allow to his/her mobile phone.

PDA vs. other mobile phone types: PDA mobile phones have separate application and communication software. Application software lies on application level and it is possible to update for a new version of personal firewall without upgrading mobile phone. In other mobile phone types these two software are not separated. That is the main reason why they are not suitable of downloading for a new version without upgrading mobile phone. The major drawback for non-PDA mobile phones is their inability to be updated for a new version of personal firewall without being upgraded. Updating for a new version is assumed to be a useful function in personal firewall and PDA mobile phones have therefore big advantage. Future will probably bring that all types of mobile phones will be developed with separate application and communication software. This will solve the problem of updating for a new version of personal firewall.

Detection intrusion attempts function in personal firewall needs support from mobile phone. In other words, mobile phone must support an updatable list of intrusion detection signatures to respond to newly discovered attacks method. List of intrusion detection signatures should be independent of mobile phone software and updating of this list should not require upgrading of mobile phone software. If the list of signatures fails to respond to newly discovered attacks methods, it would be useful to have AV protection method described in Chapter 3.1.4.

Mobile phone has to provide functionality that supports updating for a new version of personal firewall. When a new version of personal firewall is available at the operator, the user must be informed and encouraged to update it. It is then the user's responsibility to perform the update of the personal firewall for PDA mobile phones. These mobile phones allow downloading of new application software. How this operation is executed is

dependant on the underlying functionality in the mobile phone, e.g., via SMS or downloading during PDP context session.

Other mobile phone types are not suitable of downloading for a new version without upgrading software in mobile phone. Application and communication software lie on the same software. Upgrading is possible only by authorized mobile distributor. It is also possible to implement version checking of the most critical updates in the mobile phone. This could be done when e.g., the subscriber tries to activate PDP context.

Port scan is very important for collecting information of the subscriber's behaviour to be able to write correct bill. Since it costs to send blocked packets in return, it is up to user to configure rules (e.g., not answer to empty UDP packets, not answer to ICMP echo-request, etc.) in personal firewall to not send any unwanted traffic. This means that packets that may contain insecure content will be blocked and not send in return. In other words, user should not be charged for blocked packets as a result of port scanning.

For WLAN and BT, mobile phone must support MAC address authentication to get a working personal firewall. This function is used for authentication to see if two or more mobile phones are connected to the same platform.

While using Internet Explorer, mobile phone must support pop-ups filters. In this way personal firewall can decide to block or accept pop-ups that are launched using JavaScript techniques. Mobile phone must also support recognition of applications; if it is client or server initiated application.

6.1.2 Personal firewall in GGSN and in mobile phone

If personal firewall is implemented in GGSN there are few requirements mobile phone must provide to get a working personal firewall. Almost all personal firewall functions are thus done in the network by GGSN. Personal firewall in GGSN will ensure that all incoming data is authorized. In this case mobile phone should subscribe to the service in the network that provides personal firewall in the GGSN.

Mobile phone does not either need to support functions in personal firewall such as: trusted servers, trusted application etc. since these operations are done in the network. On the other hand, it is also possible for user to post-configure these functions in personal firewall. In this case, it is personal firewall in GGSN that decides which mobile phone numbers or servers the user should trust. Personal firewall should have a list of connected users e.g., Buddy list and should know which of these are on the trusted server list.

Probably the most important functionality mobile phone must provide to get a working personal firewall in GGSN is to support Traffic Flow Template (TFT). TFT is a packet filter allowing the GGSN to classify packets received from the external network into the proper PDP Context. It consists of a set of packet filters, each containing a combination of the following attributes such as: source address, subnet mask, destination and source port range, etc [34]. TFT filters traffic at the network level in GGSN. TFT includes

subnet mask and can filter based on trusted IPs. Personal firewall in GGSN includes netfilter (TFT), which should also provide that users do not receive or send unwanted traffic. TFT filters incoming traffic and trusted sites, but it is not suitable for filtering of outgoing traffic.

To be able to filter outgoing traffic as well as incoming, personal firewall should be implemented in both GGSN and mobile phone. In this way, part of personal firewall in mobile phone should handle and filter outgoing traffic. Personal firewall is split and operates in two levels: personal firewall in GGSN handles incoming traffic while personal firewall in mobile phone handles outgoing traffic, in order to prevent e.g., Trojans.

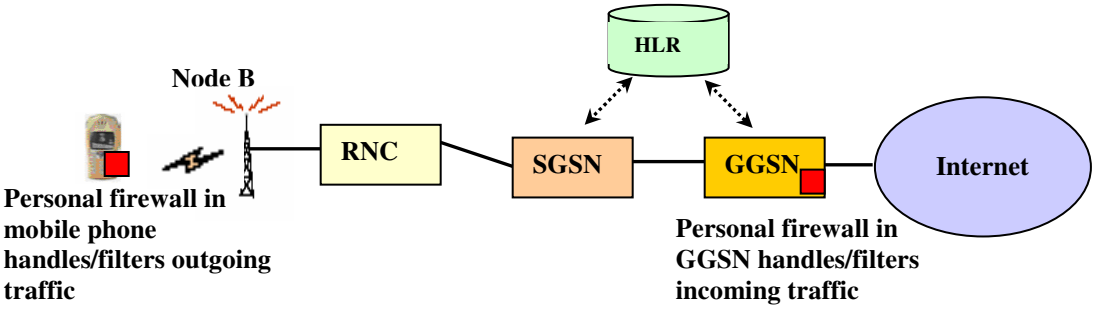


Figure 6.1 Personal firewall in GGSN and mobile phone

Mobile phone needs to support filtering functions in GGSN. Network traffic passes through the personal firewall in GGSN, which inspects every packet header. Rules for filtering of network traffic are post-configured by user or received from the mobile phone via TFT. To get working personal firewall in GGSN, mobile phone must also support PDP Context Modification Procedure.

Filtering of outgoing traffic should be based on checksum of the entire application instead of application name. This function should be supported by mobile phone since TFT is only suitable for incoming traffic from the external network, as already mentioned.

One of the great advantages in implementing personal firewall in GGSN and mobile phone is that both incoming and outgoing traffic is handled and filtered. If personal firewall is implemented only in GGSN, only incoming traffic is filtered since TFT filters traffic from the network. This is the main reason why personal firewall should be implemented in mobile phone as well, i.e. to filter outgoing traffic.

Yet another advantage of implementing personal firewall in GGSN is that it does not require upgrading of mobile phone. It is done in the network by operator. Whenever a new virus or Trojan appears in the network, the mobile phone is a tempting target for this malicious software. If the mobile user subscribes to the personal firewall in GGSN it would be the operator's responsibility to update GGSN for a new version personal firewall. The user might receive a notification when this has been done.

Alternatively, a group of users could have post-configured rules in personal firewall in GGSN that handles outgoing traffic and mobile phone must also support this function.

Functionality needed for personal firewall to inform GGSN what traffic to transmit from and to the mobile phone should be implemented. This is probably complex and expensive task because it requires developing and upgrading of personal firewall in GGSN. That is why proposed solution of spitted personal firewall (both in mobile phone and in GGSN) would gain more for both operators and users.

Disadvantage in this method of implementing personal firewall is inability to offer adequate protection in pop-ups filtering. The pop-up Java script is handled by the browser on mobile phone while personal firewall that should block or accept pop-ups is in GGSN. If mobile phone wants to download e.g., Java application that may contain pop-up Java script from the Internet it is handled by the browser. Downloading goes through personal firewall and it could come from application, site or IP that lies on trusted list in personal firewall. After downloading, personal firewall should filter these pop-ups. Unfortunately, it is not able to do this since personal firewall in GGSN cannot filter pop-ups after downloading. It should be handled by personal firewall in mobile phone which is only responsible for filtering of outgoing traffic.

Table 6.1Comparison of personal firewall implemented in mobile phone vs. GGSN

Software in mobile phone	In GGSN and mobile phone
- suitable for all connection types - configured by a user - requires update of software for all mobile phone types, except for PDA, in the case of updating for a new version	- best suitable for GPRS/UMTS - configured by a user - pre-configured by a group of users - does not require upgrading of mobile phone in the case of updating for a new version; it is done in the network by operator

Table 6.2 Functionality mobile phone must provide to get a working personal firewall

Software in mobile phone	In GGSN and mobile phone
- support servers, sites a and application mobile phone trust -support filtering incoming and outgoing traffic - support pop-up filters - support function for updating for a new version - support function that tells if application will start server or client - support authentication of applications - support updating list of intrusion detection which is independent of mobile phone software - support MAC address authentication for BT and WLAN	- must support TFT and PDP Modification Procedure - support filtering incoming and outgoing traffic - support authentication of applications - prevent that user is not charged as a result of port scanning - does not support pop-ups

6.2 Mobile phone functionality

Underlying functionality mobile phone must provide to get a personal firewall working is shown in Figure 6.1. It is presented in the sense of layers and compared to OSI reference model.

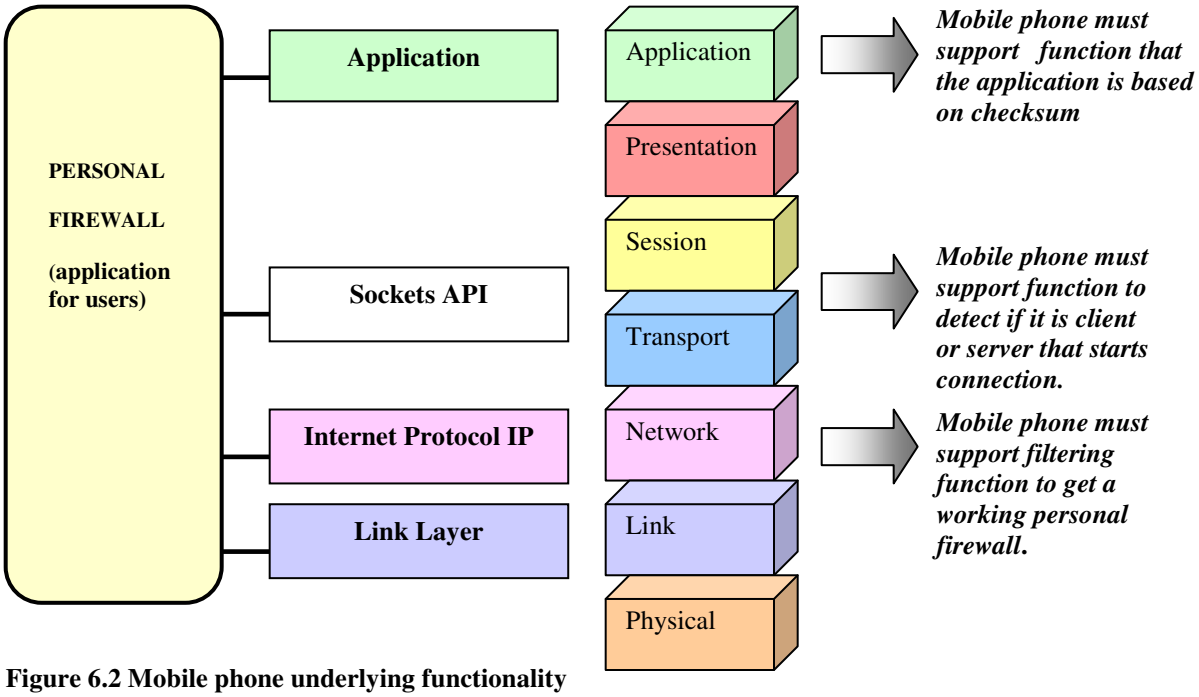


Figure 6.2 Mobile phone underlying functionality

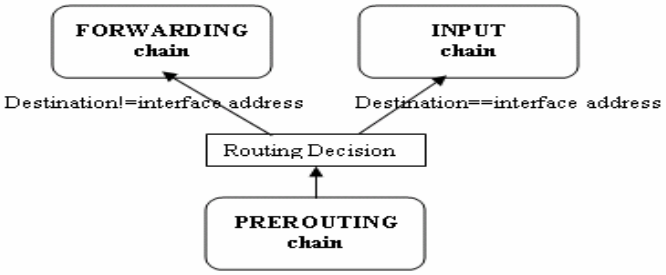
6.2.1 Link Layer and IP/TCP (UDP)

IP defines the exact format of data as it passes across the Internet and is responsible for routing of datagrams. Its main functionality is routing and filtering of packets. Filtering of packets is probably the most important function for personal firewall. Packet filtering examines IP packets and makes a decision to accept or deny traffic based upon criteria such as source and destination IP addresses and source and destination TCP/UDP port numbers. In order to provide working personal firewall, mobile phone has to support filtering functions in the Link Layer and TCP/IP.

Filtering of packets could be done in the IP. This method is similar to configuration of personal firewall for Linux [3] and it is described below. Packets traverse and are filtered in IP. Personal firewall includes netfilter and configuration tool called *iptables*[10]. The packets go through several stages and routing/filtering can be done on every stage. A chain specifies one point in the way an IP-packet takes on its way through IP layer. Every

[10] iptables includes commands and each command specifies one rule in personal firewall. Several commands in personal firewall make a chain of rules that will be traversed by each packet. Iptables has several standard built-in chains: e.g., PREROUTING, INPUT, FORWARD, OUTPUT and POSTROUTING.

table can be seen as a feature of the personal firewall. The simplest and most forward is the *filter* table. It deals, naturally, with dropping or accepting packets [3].



All packets with the destination IP matching personal firewall, will go to the INPUT chain.

All packets coming to personal firewall but with other destination address then the personal firewall itself will go to the FORWARD chain.

Figure 6.3 The forwarding chain

All incoming packets will be evaluated by the PREROUTING chains of both the *nat* (can modify source and destination information in the packet) and the *mangle* (used for advanced packet manipulation) table. Next, one looks at the source address in the header of the packet. If it is directed to the personal firewall itself, it will pass on to the different INPUT chains. Else, it is sent to the FORWARD chains, assuming that this packet is heading through the personal firewall to somewhere else. All packets leaving the personal firewall, regardless if it is forwarded traffic or it originates from the personal firewall must pass through the POSTROUTING chains where the packets can be modified before hitting the wire [3].

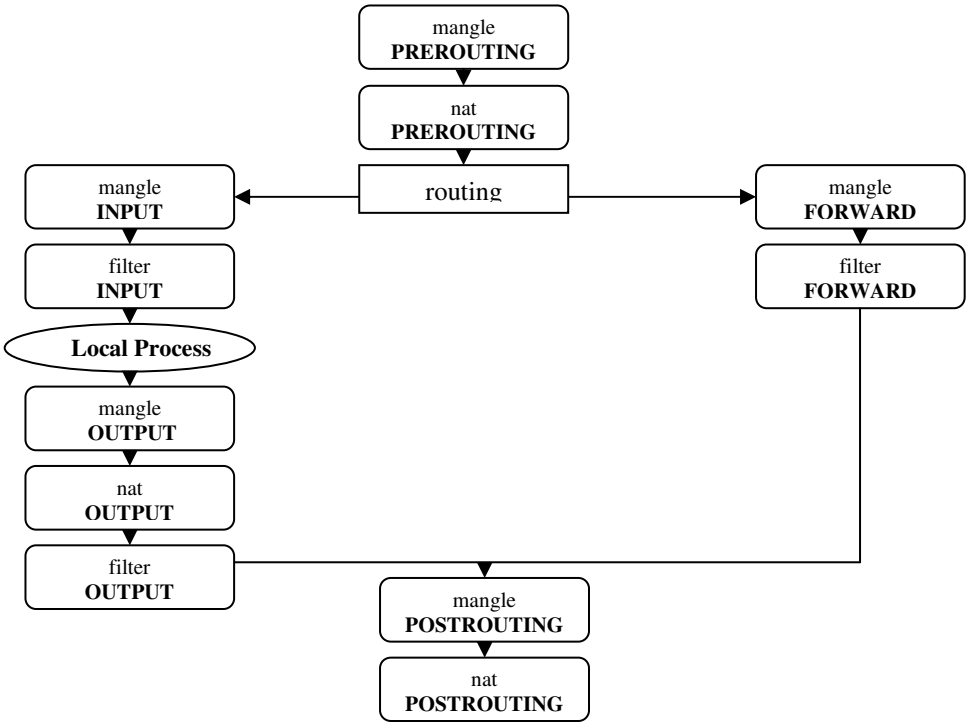


Figure 6.4 Order in which a packet traverses the different chains

Using iptables packets can be filtered based on the information in the header: Source IP, Source port number, Destination IP, Destination port number, Incoming interface, Outgoing interface, Protocol (TCP, SYN-flag, UDP, ICMP) can be filtered. The usual reaction to a packet is: Accept it, Drop it / Log it or Change header information.

Described method does filtering at the TCP/IP level, also known as network filtering. Packets traverse and are filtered in IP by netfilter and iptables. Configuration of filtering rules in personal firewall is done by the user. Packets are filtered based on header information: source and destination IP, source and destination UDP/TCP port number.

Personal firewall can also be configured to allow only trusted services to send traffic to mobile phone. This could be done by adding the rules which applications are allowed. Personal firewall also permits access to sockets only from trusted applications.

Second filtering method of configuring personal firewall is that a part of IP stack is included in personal firewall. The part of IP stack that should be included is filtering functions. In this way filtering is done in personal firewall, and does not need to go into IP layer. This could be done by implementing functions REDIRECT (ipchains)/ QUEUE (ipfilter) [35] targets in personal firewall, to get the packets at the application layer and filter them in the personal firewall instead at IP layer.

6.2.2 Socket API

A socket API (Application Programming Interface) is used to access TCP/IP networking services and create connections to processes running on other hosts. Socket provides an endpoint for communication and can be created without binding them to specific destination address.

A socket used by a server to wait for an incoming connection is called a *passive socket*, while a socket used by a client to initiate a connection is called an *active socket* [36]. In case of passive socket, the mobile phone is more vulnerable to attacks comparing to active sockets. Passive socket used by server waits for an incoming connection, so an attacker can attack mobile phone from the server. The server runs forever. It waits for a new connection on the well-known port, accepts the connection, interacts with the client, and then closes the connection. In case of active socket user (client) initiates connection. The client creates the socket, calls to connect to the server, sends requests and receives replies from the server. The only difference between active and passive socket lies in how applications use them. Mobile phone must support function to detect if it is client or server that stars connection.

Applications interact with socket interface and IP stack through a system call interface (API). To provide working personal firewall, mobile phone must support this interface functionality.

Before the socket is created, Socket layer should check in personal firewall if the application is trusted. If it is the case, personal firewall responds that it is safe to create a

socket. The socket is then created. In case personal firewall responds that this application is not on the trusted list, the application is blocked. The communication between the TCP/IP and personal firewall goes through Socket API and this might be an expensive operation and have negative impact on system performance. This is a disadvantage. In order to increase efficiency, only certain applications should be checked. This feature should be implemented as configurable in Socket layer.

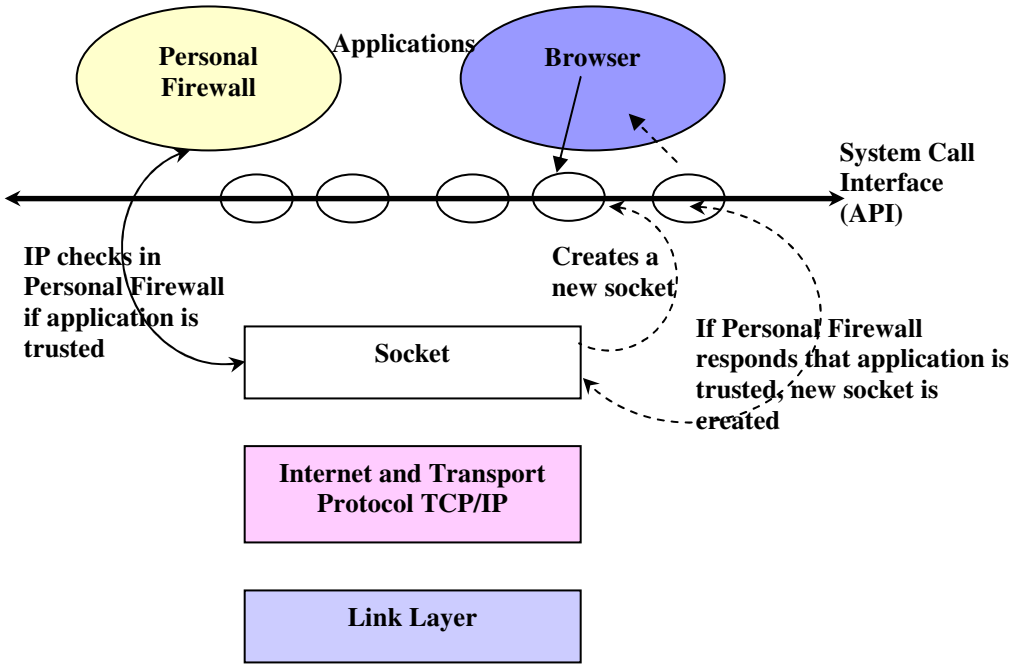


Figure 6.5 Applications interact with sockets interface and IP through an API

Personal firewall should be informed each time new socket is created for an application in order to secure mobile phone.

6.2.3 Application Level

An application level firewall evaluates network packets for valid data at the application layer before allowing a connection. Personal firewall examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. Specialized application software and proxy services are included in most application layer personal firewalls. Proxy services manage traffic through a personal firewall for a specific service such as HTTP. Proxy services can provide increased access control, details checks for valid data, and generate audit records about the traffic they transfer because the proxy services are specific to the protocol that they are designed to forward [37].

The data received is compared to the set of command rules in personal firewall and the proxy determines whether to accept or deny the packet based on the results of the rules

comparison. Based on how it is configured, the proxy may also perform other functions such as data modification, authentication logging and HTTP object caching [37].

Personal firewall can be configured to only allow web HTTP and email traffic to pass. Other TCP/IP ports, and other protocols, are routinely blocked. It has become standard practice to "tunnel" other applications through the Web ports, effectively disguised as normal Web traffic. This is generally not done for malicious reasons, but rather for pragmatic reasons, since all other ports are blocked.

Monitoring contents of packets and protocol filtering could be done at the application level. Application level filtering executes at the application level and may intercept all packets traveling to or from an application (i.e. all browser traffic). By inspecting all packets for improper contents at the application level, personal firewall can prevent the spread of e.g., viruses. Personal firewall should be aware of what traffic meant for specific applications should look like.

On the application level, mobile phone must support that filtering of incoming and outgoing traffic is based on checksum, instead of name, to prevent Trojans and attacks from external network. Mobile phone should also support filtering at the application level, e.g., HTTP error filtering. Authentication of applications should be based on checksum and mobile phone should implement this feature. Applications approved by personal firewall (authenticated by personal firewall), should go through. Otherwise, non-authenticated applications should be blocked. Mobile phone should also implement handling of unknown applications. If there are no rules for authentication of an application, personal firewall should broadcast a warning to the user about what it may be trying to do or modify. In this case, it is up to the user to decide whether to accept or block application.

Personal firewall can be configured at application level with its useful functions, as discussed several times. A big disadvantage configuring personal firewall at application layer is negative impact on system performance. Processing time is long since filtering is based on protocol and its contents, and not only header like for IP filtering.

The table below shows functionality mobile phone must provide in the sense of layers. Suggested methods of filtering are summarized in this table.

Table 6.3 Functionality mobile phone must provide in the sense of layers

IP and Link layer	Methods mobile phone must support for filtering: ▪ Filtering is done at IP Layer ▪ A part of IP stack is included in personal firewall
Sockets	▪ Mobile phone must support function that informs personal firewall each time a new socket is created ▪ Mobile phone must support list of trusted applications, sites and servers in personal firewall ▪ Communication between personal firewall and IP through API must also be supported to get a working personal firewall
Application	▪ Filtering is done at the application level based on checksum

7 Discussion

7.1 Introduction

In this master thesis, the need for personal firewall in mobile phone has been emphasized. Evaluation of different types of firewall in PC with its strengths and weaknesses were described at the beginning of the thesis, and further applied to personal firewall. Starting point for this master thesis was to look at the functions that already exist in commercial personal firewall for Windows and Linux and further suggest and discuss useful functions in personal firewall for mobile phone.

During the Internet connectivity and downloading Java applications, personal firewall plays an important role. These two mentioned scenarios need support from the personal firewall, in order to avoid mobile phone being inflected by possible virus or being attacked. Mobile phone is vulnerable to various attacks, especially during Internet connectivity. Standard mobile phone functions (WAP/WWW), mobile phone specific functions (Charging & Billing) and peer-to-peer services over IP (Push-To-Talk, Buddy List and Wireless Village) need support from the personal firewall.

Security issues in various connection types, vulnerability to attacks and personal firewall functions that might prevent and protect mobile phone from attacks were also discussed.

Last part of this master thesis was to give proposals of what underlying functionality mobile phone must provide to get a working personal firewall. Implementing personal firewall as software in mobile phone or in GGSN was also discussed. Functionality mobile phone must provide to get working personal firewall, in the sense of layers, highlighting filtering as a main function in personal firewall was emphasized.

The purpose of my work has been to see if implementation of personal firewall in mobile phone with its advantages and drawbacks is valuable and essential regarding security issues and degree of difficulty to implement personal firewall.

The discussion is structured in the same way as the main part of the report. The following issues are discussed:

- Is it essential to implement personal firewall in mobile phones?
- Should filtering of packets be done at the application or network layer?
- Suggest further work that could be done in this area.

7.2 Personal firewall in mobile phones

This master thesis mainly covers the need for personal firewall in mobile phone. Theoretically speaking, the need for personal firewall in mobile phone is essential. Personal firewall shall prevent attacks from the network, protect user during the Internet connectivity and downloading applications from the Internet. Furthermore, personal firewall shall support standard and mobile phone specific functions. Practically speaking, implementing personal firewall is a complex and expensive task. To get a working personal firewall, mobile phone must provide required functionality, which might in the other hand require upgrading of mobile phone.

An always-on Internet connection is a tempting target for an attacker and mobile phones are being more vulnerable for network attacks. One of the greatest advantages with implementing personal firewall is that it will protect mobile phone is protected during Internet connectivity. Personal firewall shall protect from attacks such as: Denial of Service, IP-spoofing and Port Scanning, as described in Chapter 4. An important drawback is that personal firewall cannot do anything to prevent Man in the middle attacks. However, it would also help in preventing billing attacks.

There are several mobile phone functions that need support from personal firewall to be able to operate in more secure way. Mobile phone standard functions such as: WAP, browsing and e-mail are dependent from personal firewall support in the same way as in PC. By implementing personal firewall, sensitive information is kept in more secure way. Sites that might include insecure content will be blocked, otherwise personal firewall shall broadcast a warning and make the user aware of what this program may be trying to modify.

More and more popular P2P services over IP; Push-To-Talk, Wireless Village and Buddy list require support from personal firewall. Personal firewall will allow traffic only from trusted lists and block any unexpected media packets. By implementing personal firewall services mentioned above will be more secure and users will also feel more secure while using them.

Personal firewall is essential in protecting mobile phone from being attacked in various connection types, as discussed in Chapter 5. It is especially useful in the case of multihoming. Personal firewall shall allow only one connection at the time to prevent IP forwarding between different connections.

Probably the weakest point in implementing personal firewall for mobile phone is the problem of upgrading mobile phone, as discussed in Chapter 6.1.1. Only PDA mobile phones have independent application and communication software, which does not require upgrading to update for a new version. Other mobile phone types need upgrading by authorized mobile distributor in the case of updating for a new version.

Another drawback is configuration issues in personal firewall in mobile phone. This could proof to be a complex task for different user groups. If personal firewall is

implemented in GGSN it is configured by the operator, with services already offered by operator. This leaves the user to pre-configure additional rules, in order to get wanted services, as discussed in Chapter 6.

All configured filtering rules may have a negative impact on system performance, especially if filtering is done at the application level. It may require some additional time to check each packet at the application level. Processing time used for filtering might also slow down other functions and operations in mobile phone.

The communication between the TCP/IP and personal firewall goes through Socket API. This might be an expensive operation and have negative impact on system performance. Therefore, only certain applications should be checked in trusted list, in order to increase efficiency.

RAM and FLASH expenses are a problem regarding implementation of personal firewall; they are limited resources and one should be careful when using these resources. When implementing personal firewall the usage of RAM and FLASH will increase. It should be one of the most important tasks to keep this usage at minimum.

7.3 Application vs. Network filtering

Filtering of packets can be done either at the application level or at the network level, as already described in Chapter 6.2. These methods of filtering will be discussed based on their strengths and weaknesses.

Network filtering can be done in two different methods, as suggested in earlier chapter. These two methods are filtering in TCP/IP layer and filtering in personal firewall that includes a part of IP stack. The most important difference of the filtering in TCP/IP layer has longer processing time compared to filtering in personal firewall that includes a part of IP stack. The disadvantage is that filtering is done at lowest layers, IP layer, while the other method goes no deeper than application level in personal firewall.

A packet filtering in IP analyzes network traffic at the transport layer and is based on information in the header. Application level filtering analyzes the complete command set for a single protocol at application space. This implies that packet filtering is faster than application filtering. This can be advantageous for personal firewall that scans for connections to web and e-mail servers, especially ones that have high amount of traffic. This is due to the fact that latency is the enemy when it comes to persons attacking user's site. Since application filtering is complete and based on the whole packet, it is slower due to inbound data being processed by the application.

Security point of view is yet another difference in filtering packets at different levels. IP filtering is less secure because it cannot inspect the network packet's application layer data. It does not keep track the state of connections, either. Still it is much faster then application level filtering that performs fewer evaluations to decide whether to pass or

block packet. IP filtering cannot monitor the contents of packets and therefore does not provide the same high level of protection as application level filtering. Further, IP filtering does not inspect the payload of the packets, only header is checked. Thus decisions whether to pass or block packets are not made based on the contents of the whole packets.

Application level filtering provides increased security then IP filtering. The disadvantage might be that it still requires extensive support from the TCP/IP and mobile phone functionality to run correctly.

Proxy services in application level filtering enforce high-level protocols, such as HTTP. Information about the communication parts passing through personal firewall server is maintained by the proxy service. It can permit access to certain network services, while denying access to others.

Personal firewall based on IP filtering run usually on an access control list and does not provide the same protection as application level filtering. This control list verifies if the destination and source addresses are legitimate. If the user is trying to scan for vulnerability in the data itself, it may cause a problem. In contrary, application level filtering permits no traffic directly between networks, and does perform logging and auditing of traffic passing trough. Application level filtering can do a large amount of logging, which makes it easier to track when a potential vulnerability happens. This could also be seen as disadvantage since large amount of logging requires resources for processing.

Another advantage of filtering at the application level is that this kind of filtering could support the ability to report to intrusion detection, which is discussed to be a useful function in personal firewall. This allows scan for patterns of network traffic that indicate known attack. Again, one should be careful since it requires additional resources.

Network filtering personal firewall is sensitive to attacks such as: IP spoofing and ICMP tunneling. In IP spoofing attacks, source or destination addresses are modified. Network personal firewall filters based only on the header information and if attacker manages to modify source address that personal firewall will trust, mobile phone is being attacked. ICMP tunneling allows a hacker to insert his data into a legitimate ICMP packet. Since the network filtering personal firewall cannot check the packet past the IP headers, it cannot deny the connection. Once again, mobile phone is vulnerable to ICMP tunneling attack when using network filtering. The best solution would be to drop all ICMP traffic at personal firewall.

Application level filtering personal firewall is less vulnerable to attacks that hide data in legitimate traffic and more vulnerable to DoS attacks. Since filtering is based on the whole packet, and not only on the header information, attacker can force lot of traffic (data) to the personal firewall. This may cause that personal firewall ceases to operate or in the worst case personal firewall crashes.

7.4 Further work

There are several issues in this thesis that could be subject to further work. Further work will manly include discussed theory applied in practice. In other words, described proposals, suggestions and scenarios should be implemented and tested. Unfortunately, time did not allow me to test scenarios described in this master thesis. To keep this section short, I only briefly present some area of interest here:

- Further work could be to implement proposed useful functions in personal firewall and test to check if they are useful in mobile phone. Results will probably point several functions that are useful in personal firewall, which are not covered in this master thesis.

- An interesting point of view regarding personal firewall would be to test if proposed useful functions are adequate for virus protection and at what degree. Furthermore, implementation of AV in mobile phone could be an interesting task to discuss.

- An interesting task could be to test mobile phone vulnerability to various attacks described in Chapter 4.1.2. From the test results, one could conclude how to protect mobile phone in the better way and outline what kind of attack mobile phone is most vulnerable. Test results could probably give an idea of what personal firewall could do in the case of Man-In-The-Middle attacks. This idea could further be used to implement a useful function in personal firewall.

- Further work could also focus on testing scenarios described in Chapter 5 and what personal firewall can do to improve security in mobile phone. Probably the most interesting scenario is the case of multihoming in various connection types. Test results will probably show which functions personal firewall shall include to protect user being attack.

- Probably, one of the most interesting tasks in further work would be to implement personal firewall as software in mobile phone and in GGSN, and compare to see which one is more reasonable and less expensive. This is a complex and challenging task, which requires a lot of time and work.

8 Conclusion

In this master thesis I have evaluated the need for personal firewall in mobile phone with its strengths and weaknesses. In today's commercial products personal firewall in mobile phone does not exist. I have emphasized that implementing personal firewall may significantly ease and secure using mobile phone e.g., during Internet connectivity and downloading Java applications.

I started out with an evaluation of which personal firewall functions in PC could be useful in mobile phone's personal firewall. I then described connection between virus and personal firewall and what personal firewall can do to prevent viruses and other insecure content. I found out that personal firewall (with relevant functions) and AV would give the best protection against malicious software. When it comes to attacks from the network, personal firewall can protect to a certain level.

There are several mobile phone standard and specific functions that need support from the personal firewall, in addition to P2P services. In a chapter dealing with various connection types, I reveled that the need for the personal firewall is essential, especially in the multihoming scenario. To get a working personal firewall I pointed out what appropriate underlying functionality mobile phone must support.

The work that has been done has also shown that there is a real need for personal firewall in mobile phone. Even if implementing personal firewall is a complex task, might have negative impact on system performance, increases RAM and FLASH expenses and problems of upgrading, the need for personal firewall is much stronger. Personal firewall in mobile phone with its drawbacks gives better protection then no security at all.

Possible ways to implement personal firewall were evaluated in this master thesis. Evaluation led that personal firewall could be implemented either as a software in mobile phone for all connection types or in the GGSN and mobile phone for GPRS/UMTS. If personal firewall is implemented in mobile phone, the user makes rules for configuration. Otherwise it is operator's task to offer services in personal firewall in GGSN, while users can add several rules according to their needs.

For most of the users, personal firewall in GGSN and in mobile phone is the best choice since it is configured by operator. If the user wants to add several rules in personal firewall it can also be achieved. Users that want to configure their own rules in personal firewall and who also have adequate knowledge of setting these rules will probably choose personal firewall in mobile phone.

Filtering of packets has been evaluated in this thesis. It could be done either at the network layer or at the application level. If filtering is done in the IP layer, it is fast filtering but less secure compared to filtering at application layer which is slower but more secure. Third method suggested in Chapter 6 is done in personal firewall and includes a part of IP stack responsible for filtering. This method is faster then application

level filtering since filtering is based on header information but still not secure as application level filtering. In this method filtering is done in personal firewall, and does not need to go to the IP layer. Processing time is thus reduced.

Regarding attacks on mobile phones, application level filtering is less vulnerable to attacks comparing to network filtering. This is logical, since application level filtering is more secure method of filtering.

In the sense of different types of mobile phones, network filtering is best suitable for mobile phones that have limited CPU resources since processing time is reduced and it is faster method. Mobile phones such as PDA (separate application and communication software) have 2 CPUs and filtering should be done at application level, having in mind upgrading of personal firewall. It looks like that all types of mobile phone eventually will have separate application and communication software. This implies that the problem of upgrading mobile phone for updating for a new version (as pointed out in Chapter 7.2 as probably the weakest point) will disappear.

Abbreviations

API	Application Programming Interface
AV	Antivirus
BT	Bluetooth
CGF	Charging Gateway Functionality
CS	Circuit Switched
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CPU	Central Processing Unit
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
DoS	Denial of Service
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Locator Resource
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
ICF	Internet Connection Firewall
ICMP	Internet Control Message Protocol
IMPS	Instant Messaging and Presence Services
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
J2ME	Java2 Platform Micro Edition
LAN	Local Area Network
MAC	Media Access Protocol
MIDP	Mobile Information Device Profile
MMS	Multimedia Service
MS	Mobile Station
NAT	Network Address Protocol
OSI	Open System Interconnection
P2P	Peer-To-Peer
PAN	Personal Area Network
PDA	Personal Digital Assistants
PDP	Packet Data Protocol
POP	Post Office Protocol
PTT	Push-To-Talk
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Message Transport Protocol

SSL	Secure Socket Layer
TCP	Transport Control Protocol
TFT	Traffic Flow Template
TLS	Transport Layer Security
UDP	Usage Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URL	Uniform Resource Locator
VAS	Value Added Services
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEP	Wired Encryption Privacy
WLAN	Wireless Local Access Network
WML	Wireless Markup Language
WV	Wireless Village
WWW	World Wide Web

References

[1] The MOREnet web page, Missouri Research & Education Network, *An Introduction to Network Firewalls and the Firewall Selection Process* Available from: http://www.more.net/technical/netserv/tcpip/firewalls/ [Accessed January 23, 2004].

[2] The VICOMSOFT web page, *Firewall White Paper* Available from: http://www.firewall-software.com/firewall_faqs/firewallqa.pdf [Accessed January 30, 2004]

[3] Kyrre Begnum, Hårek Haugerud, *Intrusion detection and firewall security* Available from: http://www.iu.hio.no/teaching/materials/MS004A/index.phtml [Accessed February 02, 2004]

[4] NORMAN, *Focuses on antivirus, antispam and personal firewall software* Available from: http://www.norman.com/products_npf_features.shtml [Accessed February 08, 2004]

[5] Microsoft, *Features of Personal Firewall* Available from: http://www.microsoft.com [Accessed February 12, 2004]

[6] Symbian, *Symbian OS – the mobile operating system* Available from: http://www.symbian.com/ [Accessed May 26, 2004]

[7] The Phone Content web page, *Virus bombards mobile phones* Available from: http://www.phonecontent.com/bm/news/gnews/phonevirus.shtml [Accessed February 18, 2004]

[8] The F-Secure web page, *Blender Threats – How To Combat Them, White paper* Available from: http://www.f-secure.com/products/white-papers/blended-threats-whitepaper.pdf [Accessed February 20, 2004]

[9] Available from: http://www.digitalworld.co.uk/index.cfm?go=buyingGuides.antivirus&page=2 [Accessed February 22, 2004]

[10] Evan Hansen, *New email virus bombards mobile phone users, News* Available from: http://news.com.com/2100-1023-241489.html?legacy=cnet [Accessed February 27, 2004]

[11] The Symantec web page, *Mobile phone Virus Hoax* Available from: http://www.symantec.com/avcenter/venc/data/mobile-phone-hoax.html [Accessed March 01, 2004]

[12] The Symbian web page, *SymbianDevZone Press*
Available from: http://www.symbianone.com/news/110303_1.html [Accessed March 02, 2004]

[13] Bruce Schneier, *Secrets & Lies, Digital Security in a Networked World*

[14] Limor Elbaz, Discretix Technologies Ltd., *Using PKC in Mobile Phones, White Paper,* Available from:
http://www.discretix.com/PDF/Using%20Public%20Key%20Cryptography%20in%20Mobile%20Phones.pdf [Accessed March 02, 2004]

[15] RFC 2786, RFC 2786 - Diffie-Helman USM Key Management Information Base and Textual Convention
Available from: http://www.faqs.org/rfcs/rfc2786.html [Accessed March 03, 2004]

[16] Available from: http://www.faqs.org/rfcs/rfc2786.html [Accessed March 03, 2004]

[17] University of Albany, *Course in acc661*
Available from: http://www.albany.edu/acc/courses/acc661/spring2002/30 [Accessed March 04, 2004]

[18] Prabhaker Mateti, *Wright State University Dayton*, *Ohio*; *Port Scanning*
Available from: http://www.cs.wright.edu/~pmateti/Courses/499/Probing/ [Accessed March 28, 2004]

[19] Dr. Steve G. Belovich, *Firewall Fairytales*
Available from: http://www.smart- data.com/seminar_docs/fw_fairytales_05_2003.pdf [Accessed March 27, 2004]

[20] Hannu u H. Kari, *HUT/ISE*, *Billing and Charging GPRS,* Available from:
http://www.cs.hut.fi/~hhk/GPRS/lect/billing_charging/ppframe.htm [Accessed March 08, 2004]

[21] The Phone Scoop web page, *Push-To-Talk*
Available from: http://www.phonescoop.com/glossary/term.php?fid=51 [Accessed March 12, 2004]

[22] The Mobile in a Minute web page, *Push-To-Talk*
Available from: http://www.mobilein.com/push_to_talk.htm [Accessed March 14, 2004]

[23] Olle Westerberg, inGate, SIP Security & Firewalls,
Available from: http://www.scmagazine.com/offline_hbpl/misc/mcs/whitepapers/SIP%20security%20and%20firewalls.pdf [Accessed April 06, 2004]

[24] The Mobile IMPS Initiative, *The Wireless Village Initiative, White paper,* Available from: http://www.openmobilealliance.org/WirelessVillage/docs/WV_White_Paper.pdf [Accessed March 10, 2004]

[25] Harri Hansen, *Department of Computer Science and Engineering, Helsinki University of Technology, Security of Mobile Systems (course Tik-110.498)* Available from: http://www.hut.fi/~hansen/papers/user-secu/#3.2 [Accessed March 11, 2004]

[26] The MeT web page, *Press Releases, INDUSTRY SPECIFICATIONS AND ROAD MAP READY FOR SECURE MOBILE TRANSACTIONS*, Available from: http://www.mobiletransaction.org/pressreleases/january220103.html [Accessed March 11, 2004]

[27] Sun Microsystems, *Java Technology -Java 2 Platform, Micro Edition (J2ME)* Available from: http://java.sun .com/j2me/j2me-ds.pdf [Accessed March 17, 2004].

[28] Sun Microsystems, *J2ME - Mobile Information Device Profile (MIDP)* Available from: http://java.sun.com/products/midp/midp-ds.pdf [Accessed March 18, 2004].

[29] Catharina Candolin and Janne Lundberg, *Attacks on GPRS, White Paper* Available from: http://www.tml.hut.fi/~candolin/studies/hakkeri/ [Accessed April, 24, 2004]

[30] Knowledge System UK, *Wireless LAN Security Issues* Avalilable from: http://www.ksys.info/wlan_security_issues.html [Accessed April 13, 2004]

[31] Wireless LAN Security, *The issues and some solutions, White Paper* Available from: http://www.advance7.co.uk/whitepapers/WLAN-Security.html [Accessed April 13, 2004]

[32] Thomas G. Xydis Ph. D, Simon Blake-Wilson, *Security Comparison: Bluetooth Communications vs. 802.11* Available from: http://ccss.isi.edu/papers/xydis_bluetooth.pdf [Accessed April, 22, 2004]

[33] A. Veeraraghavan and A.J. Elbirt, University of Massachusetts Lowell, *Securing your Bluetooth devices* Available from: http://www.computerworld.com/mobiletopics/mobile/story/0,10801,89495,00.html [Accessed April 22, 2004]

[34] UMTS and IPv6 rev3 for IPNG, *Presentations*
Available from: http://playground.sun.com/pub/ipng/html/presentations/May2001/UMTS_IPv6_rev3_IPNG.pdf [Accessed May 03, 2004]

[35] Available from: http://www.uwsg.iu.edu/hypermail/linux/kernel/0204.2/0296.html [Accessed May 07, 2004]

[36] Douglas E. Comer and David L. Stevens, *Internetworking with TCP/IP*, Volume III, CLIENT.SERVER PROGRAMMING AND APPLICATIONS

[37] Ernest Romanofski, *A Comparison of Packet Filtering Vs Application Level Firewall Technology*
Available from: http://www.group1ifw.com/whitepapers/a_comparison.htm [Accessed May 10, 2004]

Appendix A – Types of firewalls

Filter-Based Firewalls

Filter- based firewalls are the simplest and most widely deployed types of firewalls. Packet filtering does exactly what its name implies; it filters packet. Firewalls are configured with a table of addresses that characterize the packet they will, packets that will and not will be forwarded. In this context address means more than just the destination's IP address. Generally, each entry in the table is a 4-tuple: it gives the IP address and TCP (or UDP) port number for both the source and destination.

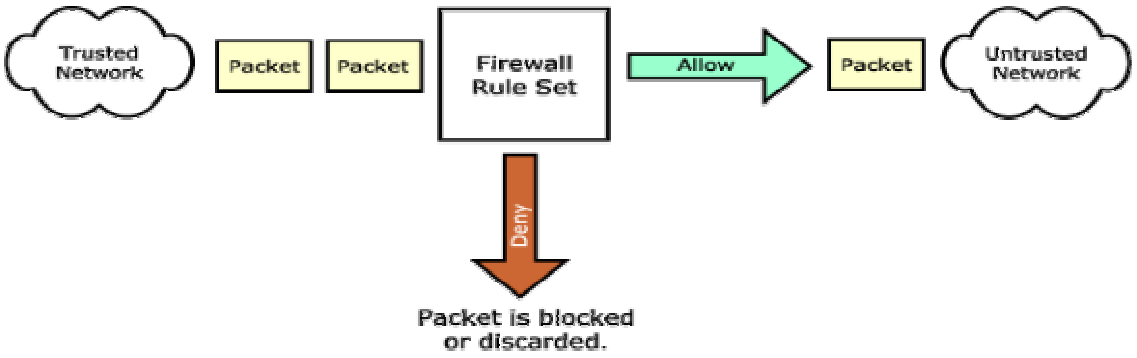


Figure A.1 Filter-Based Firewall

Strengths

- Packet filtering is faster than other packet screening methods. Since packet filtering is done at the lower levels of the OSI model, the time it takes to process a packet is much quicker. When implemented correctly, packet filtering firewalls have very little impact on overall network performance.

- Packet filtering firewalls can be implemented transparently and require no additional configuration for clients. The only indication users may have that a firewall exists, is the inability to get to a resource or service that has been blocked.

- Packet filtering firewalls are often less expensive. Many hardware devices and software packets have packet filtering features included as part of their standard package.

- Packet filtering firewalls scale better than other types of firewalls. This can be accounted for by the fact that they do not have the processing overhead that other types of firewall have.

- Packet filtering firewalls are application independent. Decisions are based on information contained in the packet's header and not on information that relates to a specific application.

Weaknesses

- Packet filtering firewalls allow a direct connection to be made between the two endpoints. Although this type of packet screening is configured to allow or deny traffic between two networks, the client/server model is never broken.

- Packet filtering firewalls are fast and have no impact on network performance, but it is usually an all-or-nothing approach. If ports are open, they are open to all traffic passing through that port, which in effect leaves a security hole in the network it protects.

- Defining rules and filters on a packet filtering firewall can be a complex task. In some cases, the task of configuring rules or filters may become so complicated that implementation becomes impossible. Lengthy access rules or filters can have a negative impact on network performance and be prone to error. As the number of rules or filters increases, so does the amount of time it takes the firewall to make comparison decisions and the chance that an inaccurate rule or filter will be added increases.

- The accuracy of rules or filters on packet filtering firewalls can be very difficult to test. Even if the rules and filters seem simple and straightforward, verifying the correctness of a rule through testing can be a time-consuming process. Sometimes testing results can be misleading and inaccurate.

- Packet filtering firewalls are prone to certain types of attacks. Since packet inspection goes no deeper than the packet header information, this method of packet screening is easier to circumvent and cannot protect against attacks directed at the application level. There are three common exploits to which packet filtering firewalls are susceptible. These are IP spoofing, buffer overruns, and ICMP tunneling. *IP spoofing* is sending the data and faking a source address that the firewall will trust. *Buffer overruns* occur when data sizes inside a buffer exceed what was allotted. *ICMP tunneling* allows a hacker to insert data into a legitimate ICMP packet. These types of attack will be described in more detail in Chapter 4.

Proxy-Based Firewall

A proxy is considered to be probably the most complex packet screening method. This type of firewall is usually implemented on a secure host system configured with two network interfaces. The proxy acts as an intermediary between the two endpoints. This packet screening method actually breaks the client/server model in that two connections are required: one from the source to the gateway/proxy and one from the gateway/proxy to the destination. Each endpoint can only communicate with the other by going through the gateway/proxy, as illustrated in Figure A.2.

A proxy firewall operates in the following manner. When a client issues a request from the untrusted network, a connection is established with the gateway/proxy. The proxy determines if the request is valid (by comparing it to any rules or filters) and then sends a new request on behalf of the client to the destination. By using this method, a direct connection is never made from the trusted network to the untrusted network and the request appears to have originated from the gateway/proxy.

The request is answered in the same manner. The response is sent back to the gateway/proxy, which determines if it is valid and then sends it on to the client. By breaking the client/server model, this type of firewall can effectively hide the trusted network from the untrusted network. It is important to note that the gateway/proxy actually builds a new request, only copying known acceptable commands before sending it on to the destination.

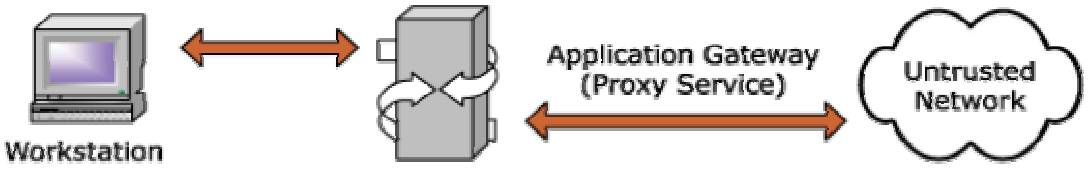


Figure A.2 Proxy-Based Firewall

Unlike packet filtering, an application gateway/proxy can see all aspects of the application layer so it can look for more specific pieces of information. It can, for instance, tell the difference between a piece of e-mail containing text and a piece of e-mail containing a graphic image, or the difference between a webpage using Java and a webpage without. From a security standpoint, the application gateway/proxy packet screening method is far superior to the other types of packet screening.

Strengths

- Application gateways/proxies do not allow a direct connection between endpoints; they actually break the client/server model. This method of packet screening truly keeps the internal and external networks separate.

- Application gateways/proxies do not route between networks. This keeps the internal network separate from the external one. Since no routing is done, this

method of packet screening inherently provides a form of Network Address Translation (NAT). Application gateways/proxies allow the network administrator to have more control over traffic passing through the firewall. They can permit or deny specific applications or specific features of an application.

- Application gateways/proxies have the best content filtering capabilities. Since they have the ability to examine the payload of the packet, they are capable of making decisions based on content.

- This type of packet screening also has extensive logging capabilities. It is capable of logging user activity and different types of traffic. This ability can provide a valuable resource when dealing with security incidents and policy implementation.

Weaknesses

- The most significant weakness of application gateways/proxies is the impact they could have on performance. Since all incoming and outgoing traffic is inspected at the application level, they are slower than packet filtering that looks at traffic at the network layer. Traffic passes through all layers until application layer where packets are being inspected. As a result, the inspection process requires more processing power and has the potential to become a bottleneck for the network.

- Another drawback of application gateways/proxies is that each protocol (HTTP, SMTP, etc.) requires its own gateway/proxy application. If it does not exist, then the corresponding protocol will not be allowed through the firewall. In addition, since each protocol requires its own gateway/proxy, support for new applications can become a problem.

- Application gateways/proxies require additional client configuration. Clients on the network may require specialized software or configuration changes to be able to connect to the application gateway/proxy. This can have quite an impact on larger networks with a large number of clients.

- Scalability can be an issue with application gateways/proxies when they are installed in large networks. Performance degrades when the number of clients increase or the number of gateways/proxies located on any one host system increases.

- Application gateways/proxies installed on general-purpose operating systems are vulnerable to the security loopholes of the underlying system. If the underlying system is not secure, the firewall is not secure.

Stateful Packet Inspection Based Firewall

Stateful packet inspection uses the same fundamental packet screening technique that packet filtering does. In addition, it examines the packet header information from the network layer of the OSI model to the application layer to verify that the packet is part of a legitimate connection and the protocols are behaving as expected.

The stateful packet inspection process is accomplished as in the following manner, as illustrated in Figure A.3. As packets pass through the firewall, packet header information is examined and fed into a dynamic state table where it is stored. The packets are compared to pre-configured rules or filters and decisions to allow or deny packets are made based on the results of the comparison. The data in the state table is then used to evaluate subsequent packets to verify that they are part of the same connection. Stateful packet inspection uses a two step process to determine whether or not packets will be allowed or denied. This method can make decisions based on one or more of the following: source IP address, destination IP address, protocol type (TCP/UDP), source port, destination port and *connection state*.

The *connection state* is derived from information gathered in previous packets. It is an essential factor in making the decision for new communication attempts. Stateful packet inspection compares the packets against the rules or filters and then checks the dynamic state table to verify that the packets are part of a valid, established connection.

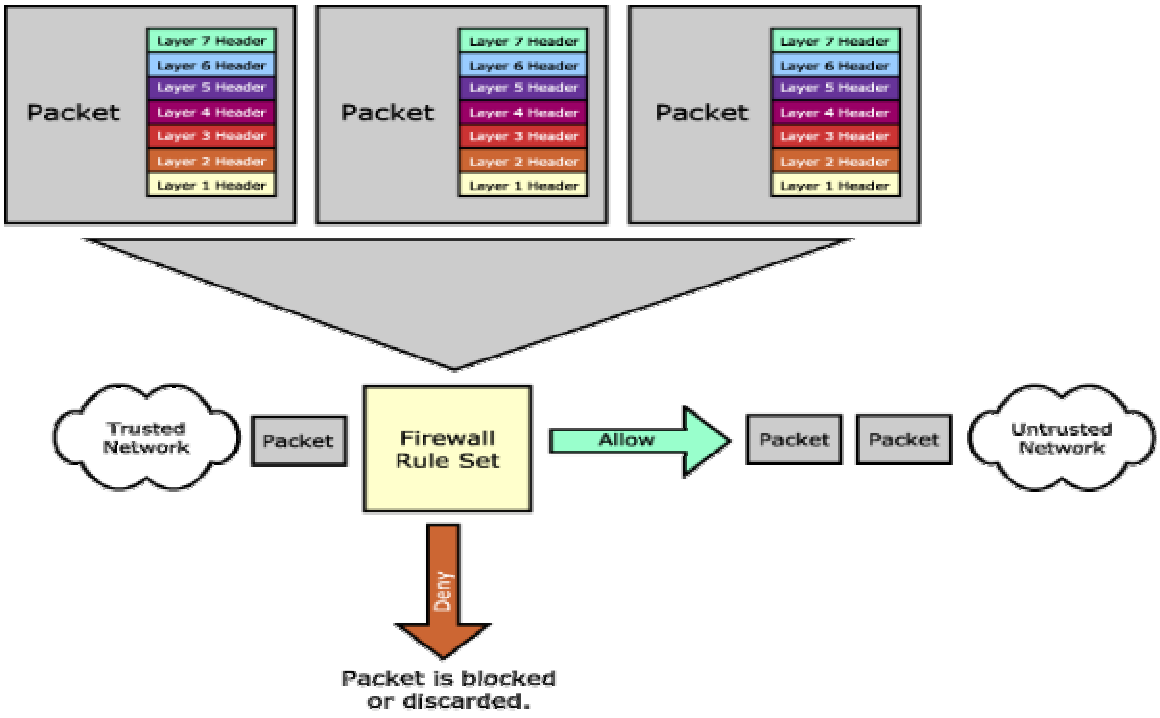


Figure A.3 Stateful Packet Inspection Firewall

Strengths

- Stateful packet inspection firewalls, like packet filtering firewalls, have little impact on network performance, can be implemented transparently and are application independent.

- Stateful packet inspection firewalls are more secure than basic packet filtering firewalls. Since stateful packet inspection digs deeper into the packet header information to determine the connection state between endpoints, it is better equipped to guard against unwanted or unauthorized access.

- Stateful packet inspection provides application layer protocol awareness. By looking deeper into the packet header information, this method of packet screening can verify that the application layer protocols are behaving as expected.

- Stateful packet inspection firewalls usually have logging capabilities. Logging can help identify and track the different types of traffic that pass though the firewall.

Weaknesses

- Like packet filtering, stateful packet inspection does not break the client/server model and therefore allows a direct connection to be made between the two endpoints.

- Rules and filters in this packet screening method can become complex, hard to manage, prone to error and difficult to test.

- Regardless of the drawbacks, stateful packet inspection does have the advantage of providing a higher degree of security by monitoring connection state information.