Requirements for Security in Home Environments

Guoyou He
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
ghe@cc.hut.fi

Abstract

Currently more and more users have more than one computer, communication equipment and peripheral facilities at home. These equipments can compose a small network via networking technologies such as Ethernet, phone-line, wireless or power-line for communicating each other and sharing resources. This network can connect to outside world through phone-line, cable modem or wireless technology. Especially, Digital Subscriber Line (DSL) and cable modem have brought home high-speed connections to Internet. Along with each of these services comes a static IP address that never changes and allows user to host their own web sites and administer their own server. However, constant connectivity to the information super-highway makes home environments easily suffering from attacks and being hacked. Further more, special features of home environment make it more vulnerable compared to other private networks. So specifying suitable requirements and policies for home networking security is critical in home networking environments. This paper analyzes the possible threats to personal home network, evaluates the risks caused by these threats, and specifies the security requirements derived from the threat analysis for home environment.

1 Introduction

With the development of modern communication and networking technology, more and more computing and communication facilities, automation equipments, and different type of networking terminals come into home all over the world. To share common resources, and fully use all the functionalities provided by these facilities, a residential home communication network can be built with different technologies. The home environment can communicate with the external world via phone line, wired LAN, wireless LAN, or mixed. The internal connection between different nodes in the home environment can also be wired or wireless.

Home networking is progressing rapidly in the internetworking field. It has introduced new features in both its communication facilities and users. In the facility aspect, some automation equipments and smart devices [16] can be connected to the home network. The security of these equipments not only has the meaning in general information security level, but also is concerned with security of home members and premises. In the user aspect, the users might be quite different from those in general corporation networks. They might be young children, people lacking security skills and the ones who do not care about security. So building and maintaining secure home network is critical for the networked homes. Following, we shall analyze and present the security objects, security threats [8] and corresponding security requirements for residential home environments.

2 Security Objectives for Residential Home Environments

The general objectives for home environments security are basically same as that of ordinary corporate networks as extracted from [8, 19] to ensure:

Confidentiality: prevention of unauthorized access to information in the system.

Integrity: prevention of unauthorized modification of information and the system including hardware and software.

Availability: prevention of unauthorized withholding or overtaking information, services and system resources.

Authenticity: assurance of the communications in the system being authentic.

Accountability: assurance of the activity of affecting the system security being traced to the responsible party.

Safety: assurance of the data and facilities being secure under the impact of system failures and adverse conditions.

Nonrepudiation: prevention of either sender or receiver from denying a transmitted data, prevention from denying of access to the system and services.

Affordability: assurance of the security features being affordable to users [17].

Access Control: prevention of unauthorized access to the system and services via communication links and terminal equipments.

3 Asset Classification

The purpose of asset classification is to ensure that each asset receives an appropriate level of protection, and is not available to unauthorized users. Different type of assets requires different type and level of protection. To be able to derive security requirements for home environments, various types of assets have to be classified and distinguished. The classified assets are listed below for home environments.

3.1 Physical and Environmental Facilities

It comprises hardware, network components, and operating locations including buildings or vehicles. The security of physical and environmental facilities is the first defense line for home environments security.

3.2 Software

It includes operating systems, network management systems, all kinds of application programs, etc. The secure operating systems are critical to the whole home environments

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

or individual component security. The security of network management and application programs can affect the security of the corresponding services or even whole system.

3.3 System Control data

It comprises the data related to access to individual workstation, automation equipment, server etc; the data related to user account management, network resource management and service profiles, which include the information related to user identity, passwords, account identity, and PIN codes, IP address, name of machines etc. This category of data should be kept confidential from outside.

3.4 User traffic data

It includes all the data transmitted over the link to and from the home environment and the data transmitted between the different nodes inside the home environment. The data could be any signaling data, system control instructs, access control messages, any user data including e-mail, fax, voice, files, and any data transactions generated by users. The public information in this category should be kept integral in its transmitting procedure. The sensitive messages should keep their confidentiality and integrity during the transaction process.

3.5 General User data

It composes of any data that is stored on the workstations, servers or portable terminals in the home environments. It can be any document regarding to career planning, health, pay, finances, e-mails, entertainment, web pages, and user's work related data etc. When this category of data transmitted over the links, it becomes user traffic data as described in 3.4. The public information in this category should keep its integrity and availability. The other user data should keep its confidentiality and integrity beyond in the storage.

4 Security Threats

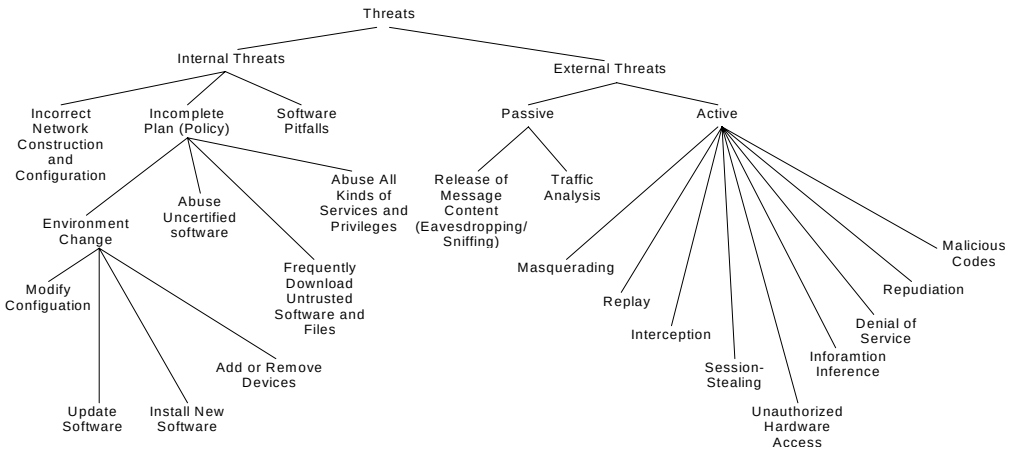

Figure 1: Overall categorization of threats

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

Residential Home Environment security threats can come from all kind of different sources, which include incorrect network building, environment changes, software security pitfalls, common security attacks, etc. The overall categorization of threats is shown in Figure 1.

4.1 Internal Threats

Internal threats are mainly classified into incorrect network construction and configuration, incomplete security plan and software pitfalls.

Incorrect Network Construction and Configuration

Incorrect network architecture design and construction, such as incorrectly arrange firewall(s), server(s), terminal equipments and other shared resources may open big security holes. Though the network is correctly constructed, incorrect configuration of firewall(s), server(s), terminals, etc. can also open security holes.

Incomplete Security Plan

Incomplete security plan mainly refers that the use of the home environments is not well planned. There is not complete security policy or no specified security plan at all in a home environment. Any member of family - your daughter, son or your children's friends can use any equipment and access any service and resource. It may cause disaster in the network system and home. The sub-items are listed following.

Intended or Unintended Changing Environment: The system administrator and users in the home intentionally or unintentionally modify the security features of the home environment may open big security holes for intruders. Modifying the configuration, updating operating system, installing new application software, and adding or removing new devices such new server, new terminals etc. can explicitly or implicitly change the home network environment and open the back door for attacking.

Abuse uncertified software: Abusing uncertified software can cause security holes mainly in four aspects: (1) user may not fully know the security features of the software; (2) the software has security pitfalls; (3) the software may embed hostile codes; (4) installation of the software may change the environment.

Frequently download untrusted software and files: The software and files from any untrusted source may contain virus and unknown hostile codes that can destroy the system and leak information.

Abuse all kinds of services and privileges by inside users: Inside users abuse all kind of available services such as downloading or playing games without restriction, access any kinds of web services, etc. Insider users abuse user privileges such as frequently removing files, changing systems setting, etc.

Using software with security pitfalls

Obviously, the back door has already been open for attacking when you use software with security pitfalls. Of course, any software might not be perfect in security. It depends how big the pitfalls are.

4.2 External Threats

The external threats are mainly classifies into passive and active attacks based on the behavior of an intruder.

Passive Attacks

Passive attacks are in the nature of Eavesdropping/Sniffing or monitoring transmissions. The purpose of the intruder is to get information that is being transmitted over the link.

Eavesdropping/Sniffing [9, 17]**:** A hacker listens and gets the user traffic or signaling message carried on the phone line, LAN, or radio wave between the home environment and outside without disturbing the conversations between correspondents. A hacker can also listen and obtain the internal wireless traffic without detection if a wireless network is employed.

Traffic analysis [19]**:** A hacker analyses the traffic between the home environment and outside by observing the time, length, source, and destination of messages to determine a home user's or mobile node's location, or to intercept important information from the transaction that is taking place. A hacker may also analyze the internal traffic of the home environment by intercept radio wave if a wireless home network is used.

Active Attacks

Active attacks involve modification of messages, interruption of data streams, and access sensitive information using various ways. It can be subdivided into following categories.

Masquerading [19, 20]: A hacker hoaxes a legitimate home user, and remote accesses to the home environment to obtain service or confidential information (e.g., a hacker exploits a legitimate user's account via Internet to penetrate the home network). The intruder may also hoax a legitimate system such as a mobile node to access the home environment, and obtain system service, operate automation equipment or get confidential information.

Replay [19]: An intruder obtains a copy of valid service request, stores it, and then replays it (e.g. if a home environment provides Mobile IP services, an individual captures a copy of Registration Request packet sent from a mobile node to its home environment, stores it, and then replay it at a later time, thereby registering a bogus care-of address for the mobile node).

Interception [19]: An intruder intercepts all the packets destined to a remote or mobile user from the home environment. As a result the authorized user can't get the services from the home network.

Session-stealing [19]: An intruder waits for a legitimate user or node to authenticate itself and to start an application, then the intruder takes over the session by impersonating the identity of the legitimate user or node (e.g., if a home environment supports Mobile IP, an intruder has physically connected to a mobile node's Ethernet-based foreign link can wait for the legitimate mobile node to register with its home agent, then floods the mobile node with nuisance packets and takes over the mobile node's session. The intruder does this by programming his network interface to use the mobile node's home address as the source address of its packets that appear to have come from the mobile node and by intercepting packets destined to the mobile node.).

Unauthorized access to hardware: An intruder uses a lost or stolen terminal equipment gaining access to home network and services. A legitimate user accesses to the critical equipments without permission.

Information Inference or Leakage [8]: A hacker sends query or signal to home environment, or directly to terminals and the automation equipments at home, observes the reaction from the home network, and deduces the information what he needs. An intruder may also obtain sensitive information through security pitfalls in the system or through deducing or searching the data stored in the system with legitimate access to the home environment.

Denial of Service: An intruder can disturb network services or traffic in different ways resulting in denial of service or reducing the availability of services. An intruder can use flooding attack sending a tremendous number of packets to the home environment. The resources are used up, the server channels are jammed, and the authorized users can't access the services in the home environment. It's one kind of denial-of-service [2, 3]. The intruder may also send countless packets to the server(s) or terminal equipments and block the internal traffic via radio wave if the wireless LAN is used inside the home.

Repudiation: It denies what a user or intruder did in the network system. It violates non-repudiation and accountability of information security. Repudiation is further divided into Repudiation of service and Repudiation message originating and receiving. Repudiation of service is that a user or intruder denies the attempts to access a service or denies the service that was provided in fact. Repudiation message originating and receiving is that a user or intruder denies that he generated or received message.

Malicious Codes [14, 15]: Virus is sensitive word for information system security. In fact, viruses are only one category of malicious codes. The threats of malicious codes to home environment may be more pervade than to corporation networks due to lacking of awareness and security facilities in a general home environment.
Malicious codes are conventionally classified as Viruses, Bacteria, Worms, Trapdoors, Logic bombs, and Trojan horses [20]. Each of them has different threat to information system security. With the lapse of time and the development of networking technology, malicious codes have shown their new characteristics and development trend. Up to date, they are mostly distributed combining network communication and multiple attacking methods. Only if they are activated, it is difficult to control their spread over the network.
Malicious codes currently are mostly distributed via software pitfalls, e-mail, network, web pages [5], instant communication tools, etc. Their behaviors can be greatly consuming system resources, destroying system seriously, distribute over the network rapidly, etc.

5 Risk Assessment

According the threat classification in chapter 4, evaluation of the threats and their possible damages caused by them are outlined in this chapter. In this assessment, the likelihood of a threat occurring is normalized as a value that ranges from 1 to 3, which means low likelihood to high likelihood. The possible loss incurred is also normalized as a value that ranges from 1 to 3, which means low loss to high loss. The *calculated risk = likelihood of the threat occurring × loss incurred*. It ranges from 1 to 9. 1 or 2 means a low risk, 3 or 4 means a moderate risk, 6 or 9 means a high risk. The moderate and high level risks in home environments are listed in Table 1.

	Threat	Assets	Likelihood	Loss Incurred	Risk
Internal	**Incorrect network construction and configuration**	Any accessible resource, software, user data, etc.	1	1 - 3	1 - 3
	Intended or unintended changing environment	Any accessible resource, software, user data, etc.	2	1 - 3	2 - 6
	Abuse services and privileges by inside users	Any accessible resource and services, software, user data, etc.	3	2 - 3	6 - 9
	Abuse uncertified software	Any accessible resource, software, user data, etc.	1	1 - 3	1 - 3
	Frequently download untrusted software and files	Any accessible resource, software, user data, etc.	2	2	4
External	**Traffic analysis**	Any user traffic information	3	2 - 3	6 - 9
	Masquerading	User traffic data, system control data, general user data.	3	1 - 2	3 - 6
	Information leakage	Any accessible resource, software, user data, etc.	2	1 - 2	2 - 4
	Unauthorized hardware access	Hardware, any accessible resource, software, user data, etc.	1	3	3
	Session-stealing	User data and accessible resources	1	2	2
	Denial of service	Available services	3	1	3
	Malicious codes	User data, system and allpication software	3	3	9
* Note: The data in this table is just my own evaluation and might not be accurate enough.					

Table 1: The moderate and high level risks

5.1 Internal Threats

Abusing services and privileges by inside users has risk level of 6 – 9. It is a high risk threat to home environments. The risk level of others varies from low to high.

Incorrect Network Construction and Configuration

It can open holes that compromise the security of the whole network. Intruders may manipulate any accessible resource or operate some terminals and automation equipments in the network. The seriousness of this threat depends on how big the security holes are. Generally, the home network should be built and configured by security professionals. The likelihood of this threat is low and assigned level 1. In case this threat happened, the loss incurred varies from level 1 to 3 with the opened security holes. The calculated risk of this threat ranges from low to moderate (1 – 3).

Incomplete Security Plan

Security plan includes the policy of using and managing the home environment. The risk caused by incomplete security plan varies with different threats.

Intended or Unintended Changing Environment: The scope of this threat can be part or whole of the home network depending on the changed security features. The environment change can be intended or unintended in the process of using the home facilities. It happens more often than the occurrence of incorrect network construction and configuration. The likelihood of this threat is assigned level 2. If this threat happened, intruders may manipulate part or all accessible resources. The loss incurred varies with change of the security features and is assigned the level 1 – 3. The calculated risk is low to high (2 – 6).

Abuse uncertified software: For convenience or temporary interest, a user might install and use uncertified software without knowing its security features. The likelihood of this threat might not be often (level 1). Uncertified software may open security holes, leak sensitive information, or destroy the system (by malicious codes), etc. The loss incurred can range from 1 – 3. The calculated risk is low to moderate (1 – 3).

Frequently download untrusted software and files: Intruders may get access to the system due to environment changes, and obtain information via embedded special code. Intruders can also use embedded code to disrupt network traffic or destroy the system. The likelihood of this threat is moderate (level 2). The loss incurred by this threat has the level 2. The risk is moderate (4).

Abuse all kinds of services and privileges by inside users: Inside user might become an inside attacker and cause security problem on the system unintentionally if he abuses any available services and user privileges. Insider users abuse privileges may weaken the system security or disturb the normal function of the system. The risk of this threat has the highest level (9).

Using software with security pitfalls

Currently, any operating system is not perfect in security. Some of them may have more pitfalls than the others. Some of them may be on the attacking focus. The damage caused by this threat might be general to an ordinary home network, but for the network containing some automation terminal equipments, it might become a high risk threat.

5.2 External threats

The risk of external threats varies a lot with the characteristics of the threats. Some the threats have high likelihood of occurring and cause high loss. Others may have very high possibility of occurring, but may only disturb the services.

Passive Attacks

Eavesdropping/Sniffing: An intruder eavesdrops on user traffic message, it may be used to access to security management data or other useful information for active attacking. This attack has moderate likelihood (level 2) and low loss incurred (level 1). It's a low risk attack.

Traffic analysis: An intruder analyses the message traffic in the wired or wireless interface to get access information. As shown in Table 1, the risk of this attack is high (6 – 9).

Active attacks

Masquerading: An intruder hoaxes an authorized user or communication node to access services, intercept user traffic, or control data on the wired or wireless interfaces. It can happen quite often (level 3). The loss incurred of this attack varies from low to moderate (1 – 2). The calculated risk varies from moderate to high (3 – 6).

Replay: This attack can be prevented using general security mechanisms. The risk of this attack is low.

Interception: An intruder may intercept user traffic temporarily. It's a general attack with low level risk.

Session-stealing: An intruder can get the privilege of legitimate user using this attack. The intruder may manipulate any available data in the system. It has low likelihood and moderate loss incurred. The risk of this attack is low.

Unauthorized access to hardware: An intruder may use a lost or stolen terminal equipment to get access to unauthorized resources. The intruder can have the privilege of legitimate user and manipulate available data. An insider user may also access to some special facilities without permission. The likelihood of this attack is generally low, but the loss incurred is high. The calculated risk is moderate.

Information Inference: An intruder deduces information from query and response to get access to the system. It's a general threat with low risk.

Information Leakage: A hacker may get sensitive information through security pitfalls or legitimate access. The intruder may manipulate any accessible data in the system. The risk of this threat is low to moderate.

Denial of Service: This attack occurs frequently, but the loss incurred is low. It's a moderate risk threat.

Repudiation: All the service activity and message transmission can be logged or traceable if the accounting system is complete in the system. The risk of this threat is low.

Malicious codes: Currently, malicious codes or viruses are the biggest threat to network security. Malicious codes can disclose information, manipulate data, and even destroy the system. This threat has the highest risk to network security.

5.3 Security Statistics

In addition to risk assessment with analysis, statistical data is the most realistic illustration of risks for security threats. A survey of 538 security professionals in U.S. corporations was done in [6], the results are given in following sections.

Attacks on the rise

The attacks reported grow rapidly in recent years. The classification of the reported attacks on the rise is shown in Figure 2.

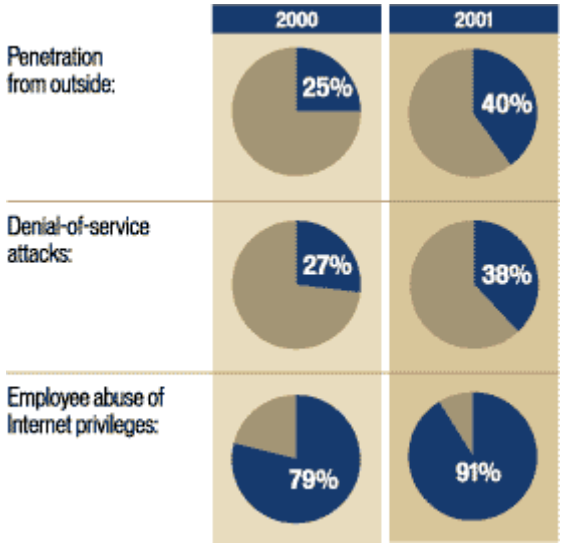

Figure 2: Attacks on the rise [6]

Virus alert

Problems caused by viruses: Server downtime increased substantially from 1999 as shown in Table 2.

	1999	2000
Server down for more than one hour	9%	64%
File problems from viruses	50%	66%
Companies with data loss	31%	40%

Table 2: Problems caused by viruses [6]

The ratio of virus to e-mail: Figure 3 plots the ratio of virus to e-mail from July 2000 to June 2001. The ratio varies from one virus in every 1,400 e-mails in September 2000 to one in every 400 in May 2001.

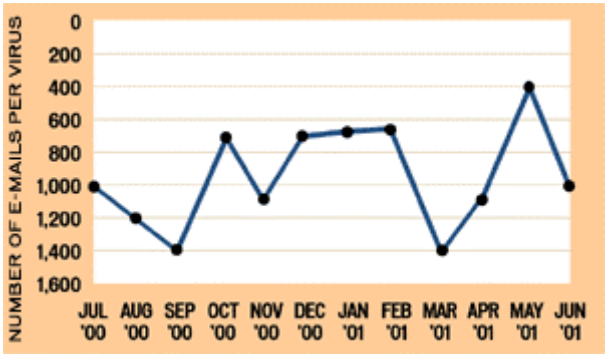

Figure 3: E-mail flu season [6]

From above analysis and statistics, we can see that inside users can cause high risk threats with abusing user privileges. The threats from insiders are increasing very fast lately. Malicious codes or viruses have the highest risk to network security. They can come from various sources. Defense against malicious codes is critical in a home environment. Masquerading and traffic analysis are the main attacks from outside users or intruders. These attacks are the main sources of the penetration from outside. They have high security risks. Mitigating these attacks is critical for defending the rising penetration from outside. Denial of service has moderate risk. However, it happened more and more frequent in recent years. The threats from denial of service are growing fast.

6 Security Requirements

According to above threat analysis, following requirements are derived. They are classified into different group as following.

6.1 Requirements on Home Environment Construction and Configuration

It is strongly recommended that all the requirements listed in this section should be fulfilled by professionals of network administration or under the supervision of network professionals.

1) *Correct design of home network architecture*: Firewall(s), server(s), terminal equipments, automation equipments, and shared resources are organized correctly.

2) *Selecting suitable operating system(s) with less security pitfalls*: The operating system should satisfy the security demand of home environment and not be on attacking focus.

3) *Selecting and using verified and authenticated application software*: It is recommended to avoid use uncertified software.

4) *Correct installation and configuration of operating system(s) and application software*: Operating systems and application programs should be correctly installed

and configured in all the nodes. Unnecessary programs should be removed from the nodes or system.

5) *Correct configuration of the system after adding/removing equipments to/from the system*: The adding/removing equipments should not weaken the security features of the system.

6) *Correct configuration of the system after installing/removing software*: it is required to installed verified and authenticated software. After the installation, the system should be correctly configured. When removing software or deleting files, correct procedure should be followed. The software/file removing should not cause any security issues in the system. The installation/un-installation of software/file should not weaken the security features of the whole and individual system.

7) *Correct configuration of the system after system updating or conversion*: The individual system, or even the whole system should be correctly configured after system updating or conversion. The system updating and conversion should not weaken the security features of the individual system and that of the whole home environment.

8) *Correctly modifying security settings*: When modifying the security settings in the system, the user should understand the effect of any change of the security features. Any unintended change should be avoided.

All above requirements are derived from the internal threats related to the network construction, configuration, and environment change. The requirements are critical for secure home environments.

6.2 Requirements on General Security Policy

1) *Correctly creating complete security policy*: The security policy should specify the rules for using the facilities in the home environment. It should specify the system administration privileges, user's rights and responsibilities, use of resources, storing sensitive information, authorization, authentication, etc. It should also guide users to correctly use the individual facility and avoid security issues.

2) *Use individual account*: Same as the user management in general LAN, each user in the home environment should be assigned to his/her own account by the system administrator.

3) *Changing security settings and the configuration is restricted*: The changing of security features and configuration is restricted to general users. Any modification of the security features should under the control of system administration. No changes on the configuration can be done for an individual system and the whole home environment before exactly knowing the effect of the changing.

4) *Avoiding download and install unverified software*: Users should be informed to know the impact of using uncertified software.

5) *Avoiding unnecessarily download files from unverified sources*: Users should be informed to know the potential impact of downloading material from unverified sources.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

6) *Avoiding to abuse users' privileges and services*: User privileges such as deleting files, removing software, changing the attributes of files, etc. should be restricted.

The requirements in this section are mainly related to the internal threats. They are also critical to the security of the home environment. It might be difficult to reach all these requirements, but reaching these requirements as many as possible can greatly mitigate the threats.

6.3 Requirements on Mitigating External Threats

1) *Ensure the sensitive traffic data integral and confidential*: It is required that the sensitive traffic data over the link (wired/wireless) should be ciphered to mitigate the threats from eavesdropping/sniffing, traffic analysis, replay and session-stealing.

2) *Ensure the remote authentication data integral, confidential and fresh*: It is required that the remote authentication data should be ciphered and variable to mitigate the threats from masquerading, replay and session-stealing.

3) *Ensure the traffic data over the internal wireless link integral and confidential*: It is required that the important traffic data such as signaling and control instructs over the internal wireless link (if it exists) should be ciphered to mitigate the threats from eavesdropping/sniffing, masquerading, traffic analysis, replay and session-stealing.

4) *Ensure the confidentiality of authentication related data*: It is required that the user authentication related data such as passwords and PINs should be confidential and difficult to figure out to mitigate the threats from unauthorized access to hardware.

5) *Keep the confidentiality of location information*: It is required that keeping location information such as IP address and e-mail address as confidential as possible to mitigate the threats from interception, information leakage, denial of service and malicious codes.

6) *Use well-known software*: It is required to choose well-known and secure software to mitigate the threats from the software pitfalls.

7) *Discard flooding packets*: It is required to filter and discard flooding packets to mitigate the threats from denial of service.

6.4 Requirements on Anti Malicious Codes

1) *Using anti virus software*: It is required to install anti virus software and update it instantly to mitigate the threats from virus.

2) *Avoid frequently download software and files from uncertified sources*: It is required to avoid download unnecessary material from unverified sources to mitigate the chance of introducing malicious codes.

3) *Avoid to open unfamiliar e-mail attachments*: It is required that users to avoid open any unfamiliar e-mail attachments.

4) *Preventing of malicious code redistribution*: In case malicious codes was detected in the system, it is required to isolate the system or equipment to prevent its further distribution.

Malicious code attack has become more and more disastrous and pervasive. Implementing the requirements on anti malicious codes is extremely important for home environment security.

6.5 Requirements on Storage of Sensitive Data

1) *Take backup to important data*: It is required to take backup for valuable data and files to avoid data loss when system collapses.

2) *Cipher critical security related data*: It is required to encrypt security related data when it is stored in the system.

3) *Cipher sensitive data*: It is required to encrypt important sensitive data when it is stored in the system to avoid information leakage.

6.6 Requirements on Detecting and Accounting of Security Violation and Reaction

1) It is possible to ensure the system can detect any security violation in the home environment.

2) It is possible to ensure that the system can take correct reaction to block or prevent the detected security violation.

3) It is possible to ensure that the system can log any security violation incident in the home environment, and make all the incidents accountable.

7 Business Aspects of Security in Home Environment

Home network is the collection of the facilities that process, store, transport and mange information. It enables the connection and integration of multiple computing, control, monitoring, communication and smart devices in home. Up to date, the rapid proliferation of personal computing devices and Internet speeds up the advancement of home networks.

7.1 Market Drivers of Home Networks [12]

The market drivers are mainly in three areas, changing the face of workplace, PC-based households, and increasing of smart devices.

Internet has made changes such as cost cutting on office rent and less travel for time saving and clean-air possible in workplace. These changes require a growing need for home network. In USA, there were 11.1 million home-based telecommuters between

1995 and 1997. The number increased to 15.7 million in 1998. Many small businesses starts from home, more the 12.6 percent of residences in U.S. run small businesses in home. These businesses need reliable home network solutions.

Investigation shows that 9.4 million U.S families have two PCs, and 3 millions have three or more till 2001. The widespread availability of PCs with cheap price makes more and more households have multiple PCs. Investigation also shows that the demand for Internet access in the home continues to grow, 22 percent of U.S. households subscribe to an on-line service or an ISP. Many of them also have additional PCs dedicated to Internet access. All these drive the demands on home networks.

With the advancement of technology, more and more smart devices have appeared. They allow users to control and monitor events in consumer-based appliances, home electronics, and home-security systems. The number of smart devices shipped surpassed that of PCs in 1999. The number of smart devices shipped continues increase to 57.5 million in U.S in 2002. As these devices become more common, the need for home networking will increase correspondingly.

7.2 Security Needs for Home Networking

With the increasing need for home network and cheap cost (starting from $15) for building a home network [11], we can predict that the home networking will be a big market in recent years, though accurate statistic data is not available yet. From the dramatic growth of number of Internet hosts and security incidents and vulnerabilities reported [1] as shown in Table 3, securing home environment has great potential for network security business.

Year	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**1999**	**2000**	**2001**
Incidents	773	1334	2334	2412	2573	2134	3734	9859	21756	52658
Vulnerabilities				171	345	311	262	417	1090	2437

Table 3: Security Incidents and vulnerabilities reported in past 10 years

Above information clearly shows that the number of security incidents and vulnerabilities are growing dramatically. We can foresee that the increment of home network comprising miscellaneous communication facilities and software will greatly contribute to the growth of the number of security incidents and vulnerabilities in the coming years.

8 Conclusion

Home networking is rapidly progressing trend in the internetworking field. Compared to a corporation network, home environment has its own special features on security requirements except the general requirements for all other private networks. On one hand, the involvement of automation equipments in home requires more demanding security requirements for a safer home. On the other hand, the home environments are less secure than corporation private networks. The main reasons for it are: (1) The network may be designed and built by non-professionals in the network and security fields. It has bigger possibility of opening security back doors for attacking. (2) The users of a home

environment are mostly not well trained. They are lacking awareness and knowledge on home networking environment. Home environments are more possibly modified both intentionally or unintentionally by their users. (3) Lacking of security professionals take care of the network security. (4) Lacking complete security policies. (5) Abuse user's privileges can frequently create security issues and make the systems malfunction. All these can easily open holes for intruders, and make the home environment more vulnerable. (6) Threats from malicious codes are becoming more and more serious for network security. Malicious codes have the highest risk to home environment security. The critical requirements on secure home environment are correct network construction and configuration, creating complete security policies, restricting abuse user's privileges, maintaining stable environment, using well functioning virus defense system and creating complete virus defense policies.

9 References

[1] Cert Coordination Center, CERT/CC Statistics 1988-2001, Jan. 10, 2002, [referred 20.02.2002]
< http://www.cert.org/stats/cert_stats.html>

[2] Cert Coordination Center, Denial of Service Attacks, Jun. 4, 2001, [referred 20.02.2002]
< http://www.cert.org/tech_tips/denial_of_service.html>

[3] Cert Coordination Center, Home Network Security, December 5, 2001, [referred 05, 02, 2002]
< http://www.cert.org/tech_tips/home_networks.html>

[4] Cert Coordination Center, Intruder Detection Checklist, Jul. 20, 1999, [referred 22.02.2002]
< http://www.cert.org/tech_tips/intruder_detection_checklist.html>

[5] Cert Coordination Center, Understanding Malicious Contents Mitigation for Web Developers, Feb. 2, 2000, [referred 22.02.2002]
< http://www.cert.org/tech_tips/malicious_code_mitigation.html>

[6] Computerworld Security Knowledge Center, Security Statistics, July 09 2001, [referred 16. 04. 2002]
<http://www.computerworld.com/itresources/rcstory/1,4167,STO62002_KEY73,00.html>

[7] Cooper Frederic J., Coggans Chris, etc., Implementing Internet Security, New Riders Publishing, 1995.

[8] Gollmann Dieter, Computer Security, John Wiley & Sons, England, 1999, ISBN 0-471-97844-2.

[9] Graham Robert, Sniffing (network wiretap, sniffer) FAQ, April 15, 2000, [referred 20.02.2002]
< http://secinf.net/info/misc/sniffingfaq.html>

[10] Hayes Keith, Active Security Monitoring and Containment with Cross Technology Correlation: The Next Generation in Computer Security Technology, Feb 11, 2002, [referred 20.02.2002]
< http://online.securityfocus.com/guest/10414>

[11] HomePCnetwork, FQA, June 09, 2001 [referred 20.02.2002]
<http://www.howstuffworks.com/framed.htm?parent=homenetwork.htm&url=http://www.homepcnetwork.com>

[12] Internet Engineering Consortium, Home Networking, 2002, [referred 25.03. 2002]
< http://www.iec.org/online/tutorials/home_net/>

[13] Joe Runnebaum, The Need for Multi-layered Defenses on the Personal PC, November 28, 2000, [referred 05, 04, 2002]
< http://rr.sans.org/homeoffice/defenses.php>

[14] Marcel Dekker, Security of the Internet, New York, 1997 [referred 05, 02, 2002]
< http://www.cert.org/encyc_article/tocencyc.html>

[15] Matthew J. Brodeur, Security Concerns In Home Automation Technologies, June, 27 2001, [referred 05.02.2002]
< http://rr.sans.org/homeoffice/auto_tech.php>

[16] Patria Leath, Addressing and Implementing Computer Security for a Small Branch Office, October 10, 2001, [05.04.2002]
< http://rr.sans.org/homeoffice/branch.php>

[17] SANS Institute resources, Essential Security Actions: Step by Step, 21.08.2001, [referred 04.02.2002]
<http://www.sans.org/newlook/resources/esa.htm>

[18] Solomon James D., Mobile IP the Internet Unplugged, Prentice Hall PTR, 1998.

[19] Stallings William, Network Security Essentials: Applications and Standards, Prentice Hall, 2000.

[20] Vincent Vono, A General Overview of Attack Methods, June 25, 2001, [referred 04.02.2002]
< http://rr.sans.org/threats/attack_methods.php>