Local and Public Traffic Concrete Barrier *(TCB)*

Tech. Ass. Ali Abdul Hussien Abdul Wahed

Computer Department. Education Collage for Girls. Kufa University

Abstract

This research presents the Local and Public Traffic Concrete Barrier software (TCB) which work as a first defensive line to the computer from any remotely or locally attackers or intruders. The key feature in the TCB software that it does not depend or use the built in windows firewall which is became week against the new attacking techniques. The TCB software can blocks all TCP process based on rules that can be specified and saved by the user such as base on Process Name, Remote IP or Remote/Local Port. In order to make the user rules unchangeable the TCB is password protected software with 3 different security levels and it can also Logs and save all the activity. Depending on the user defined rules the TCB act like a Virus/Spyware/Adware basic protector that alerts the user when it's automatically scans any Processes, IP or Port that matches with the user preset rules. All the above mentioned TCB capabilities and features helps to keep the computer more secure. As well it restricts information that comes to the computer from other computers, providing more control over the data on the computer and providing a line of defense against people or programs (including viruses and worms) that attempts to connect to the computer without invitation (unsolicited request).

Introduction

Day after day the security of the local/public traffic that transforms through the intranet/internet became more essential and important, especially for the vital information that always targeted by the attackers.

A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. [1].

A firewall also provides the ability to control access to site systems. For example, some hosts can be made reachable from outside networks, whereas others can be effectively sealed off from unwanted access. A site could prevent outside access to its hosts except for special cases such as mail servers or information servers. [2]

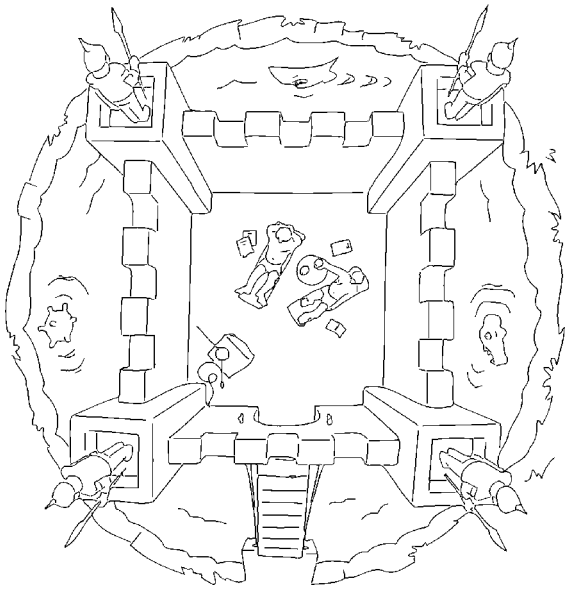

Figure 1- Firewall acting as a protected

This brings to the fore an access policy that firewalls are particularly adept at enforcing: do not provide access to hosts or services that do not require access. Put differently, why provide access to hosts and services that could be exploited by attackers when the access is not used or required? If, for example, a user requires little or no network access to her desktop workstation, then a firewall can enforce this policy. [3].

Firewall Concepts

There are two basic ways to create firewall rule sets: “inclusive” or “exclusive”. An exclusive firewall allows all traffic through except for the traffic matching the rule set. An inclusive firewall does the reverse. It only allows traffic matching the rules through and blocks everything else.

Inclusive firewalls are generally safer than exclusive firewalls because they significantly reduce the risk of allowing unwanted traffic to pass through the firewall. [3].

Windows XP Firewall Limitations

Although the Windows XP firewall will work fine in some situations, its default setting is to block only "incoming" intrusion attempts; it’s a basic firewall. [4]

TCB software has the ability to block both "incoming" intrusions and "outgoing" attempts to access the internet by various programs. Blocking outgoing attempts will immediately notify the user should you have

an unwanted Trojan/spyware that's trying to "phone home". Although there are ways to create similar blocks from within the Windows Firewall, it takes manual configuration. Basically, TCB software is easier to configure for this purpose.

Designing Goals in the TCB software

The major goal of the TCB was to cover the limitations in the slandered windows firewall and that through designing and implement the following key features:

1. TCB does not depend or use the built in windows firewall which is became week against the new attacking techniques.
2. The TCB software can blocks all incoming or outgoing TCP/IP process based on rules that can be specified and saved by the user such as base on Process Name, Remote IP or Remote/Local Port.
3. TCB is password protected software with 3 different security levels and it can also Logs and save all the activity.
4. Depending on the user defined rules the TCB act like a Virus / Spyware/ Adware basic protector that alerts the user when it's automatically scans any Processes, IP or Port that matches with the user preset rules.

All these abilities were designed and programmed using Visual Basic Ver. 6.0 taking advantage of its Application Programming Interface *(API)*, the API facilitate controlling and manipulating Windows Registry and dynamic link libraries files (DLL) which it controlling Windows task manager and have the ability to controlling the computer incoming traffic through controlling the remote IP or Port and controlling the outgoing traffic through controlling the process that want to communicate with the external network.

Figure 2 - Traffic Concrete Barrier TCB

TCP Software Mechanism

TCP software is a user defined firewall with advanced features that enable the user to block any suspicious process from any file or any port connected to the TCB system, its mechanism depend on the indicated selections by the user regarding the file names or process name that attempt to manipulate the system through its Registry keys and values in additional to mark any port as a dangers or safe information source and that gave the ability for block or allow the current activity.

TCB mechanism can be illustrated through below steps:

1- Secure the user process or ports blocking or allowing selection and setting from any unauthenticated or unauthorized modifier through:

A. Make the TCB totally isolated from the current system in controlling and administrations regards, which implemented in the TCB through making its model un modifiable and not changeable except from the authorized user.

B. The authorization is controlled through a multiple security level password as below:

Security Level 1 (Low): this level is only protecting the TCB software Enable / Disable Function.

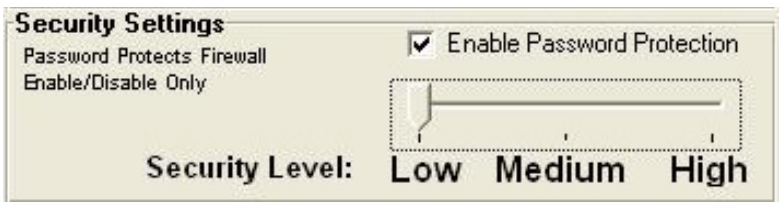

Figure- 3- Low Level Security

I. Security Level 1 (Medium): this level protect the User defined Rules and options Editing.

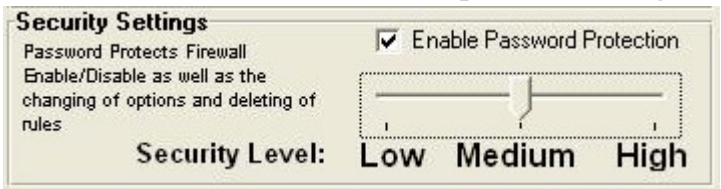

Figure 4- Medium Level Security

I. Security Level 1 (High): this level protects all TCB functions.

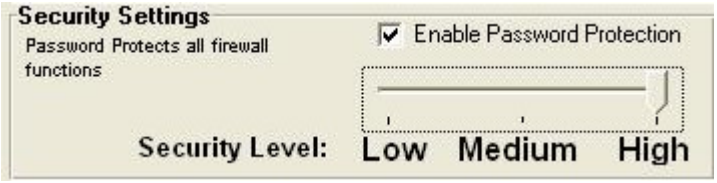

Figure 5- High Level Security

TCB default security level is Low.

2- In real time manner the TCB will cross-check the windows Task Manger with the already set process or ports list and take a decision regarding its activity wither its allowed or blocked according to the user identifications, this outcome is depend on registry manipulation through the TCB and that by using Visual Basic Application Programming Interface that facilitate this process using the Administration privileges.

3- In case that the current process is attempt to make a Registry manipulating activity and its name is set by the user in the blocked list then the TCB will kill this process and that through using the End Process Tree Instruction through calling its registry API, then TCB will informed the user about this blocked process through an alarm message.

4- The function of cross check between the current process and the process in the allowed and blocked list will be functional all the time the TCB is running in order to earn the user the first alarm barrier system.

TCB Algorithm:

1- **TCB Initialization:** initialize all the interface components and DLL files through the API instructions in order to activate the functionality of all TCB processes.

2- **Registry Connecting and Initialization**: through this step TCB will connect to the system registry and initialize and create the necessary new registries in order to make the TCB isolated from the current system and out of controlling any intruder or modifier.

Password Checking: after opining TCB interface the password security level will be checked according to the user configuration that is stored in the new TCB registry named TCBPWD01.

3- **Utilizing DLL Files and Enumerating:** in this step TCB will scan all the current processes information (process ID, Process name, port, handle) from the task manager in the same system, these captured process will be stored in the new TCB registry named PINFO and that through utilizing the DLL files and registries which initialized in the first step.

4- Creating/Checking Rules: in this step the user can set a new rules, delete and modify all the configuration regarding the blocked or allowed list of activities, also if the user already did these configuration then TCB will cross- check the recorded PINFO with the blocked list and decide to kill or allow the process in his activity.

In order to makes TCB steps more clear and obvious, the below flowchart briefly explaining and describing its major structure.

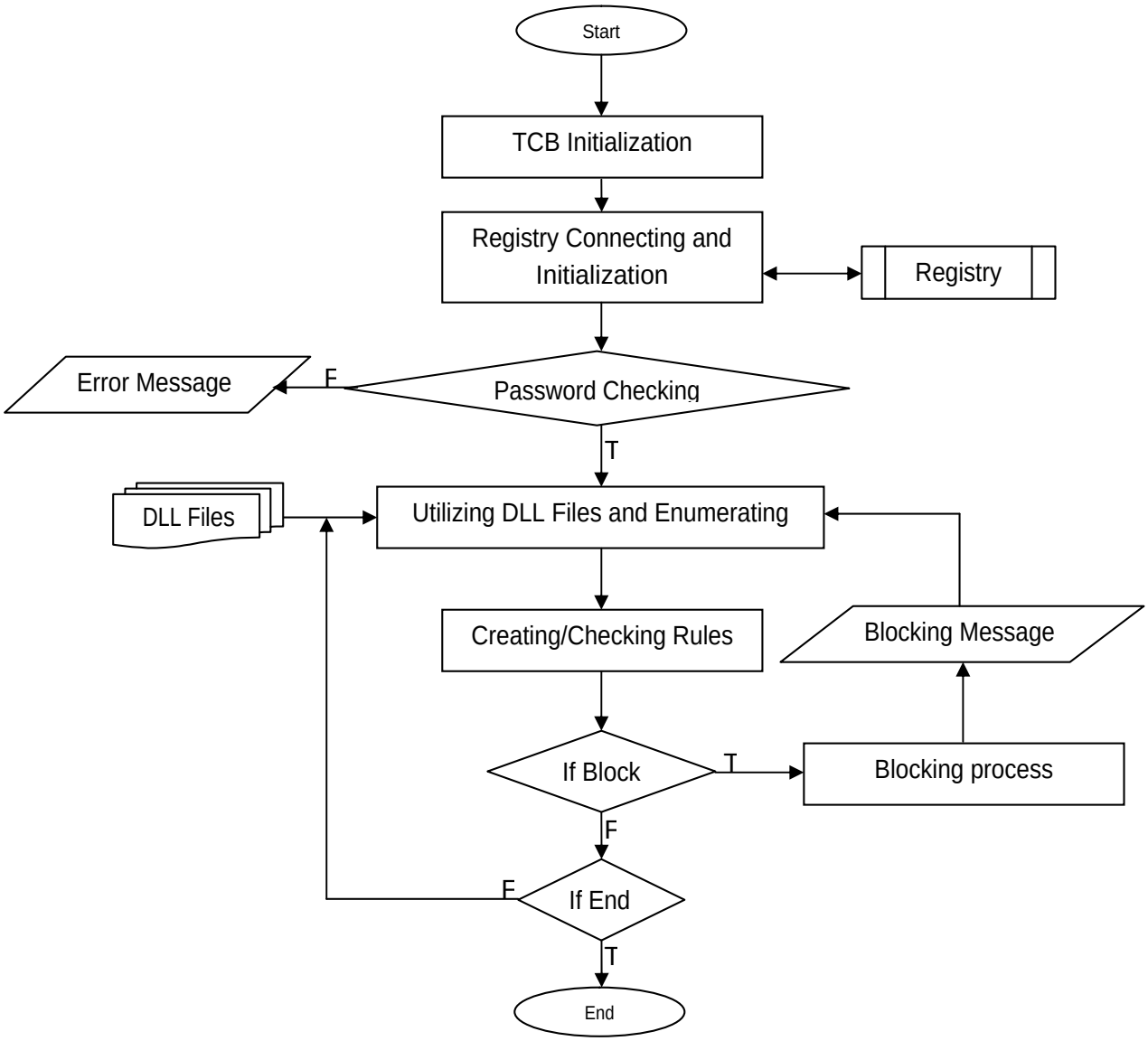

Figure 6- Traffic Concrete Barrier TCB Flowchart

TCB Interfaces

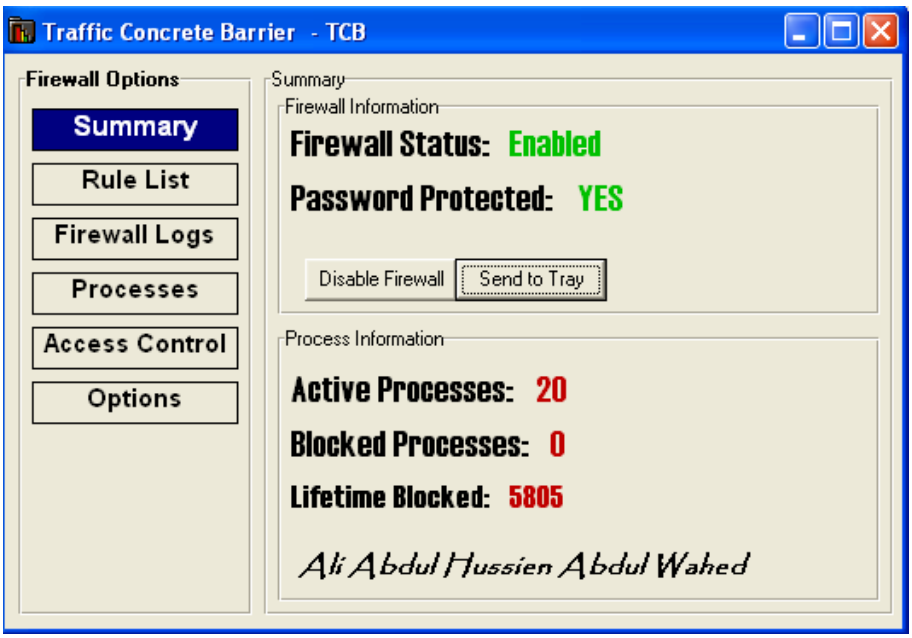

Figure 7 - Main TCB Interface - Summary Tab

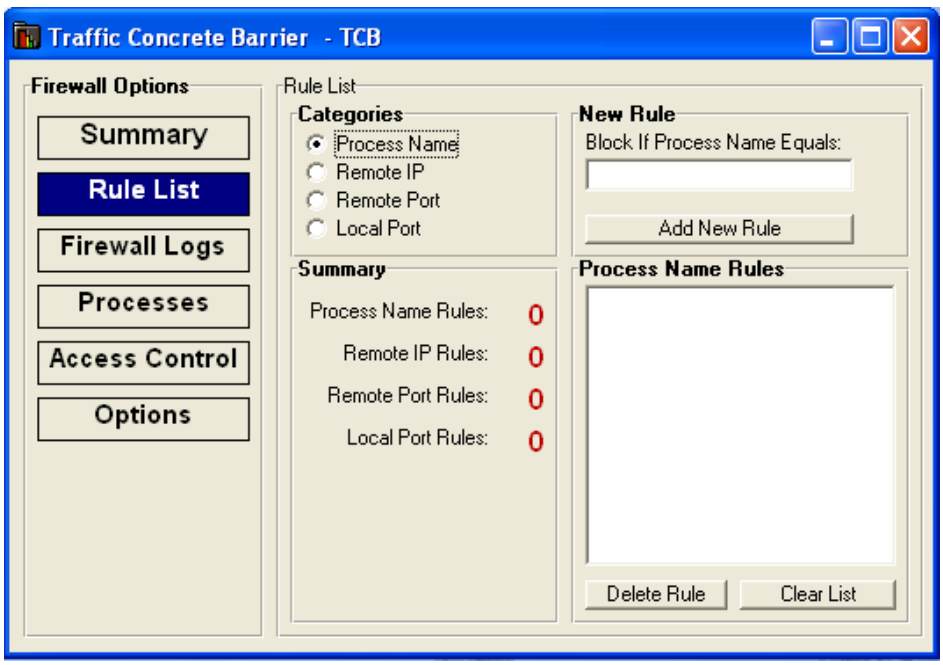

Figure 8- TCB Rules Tab

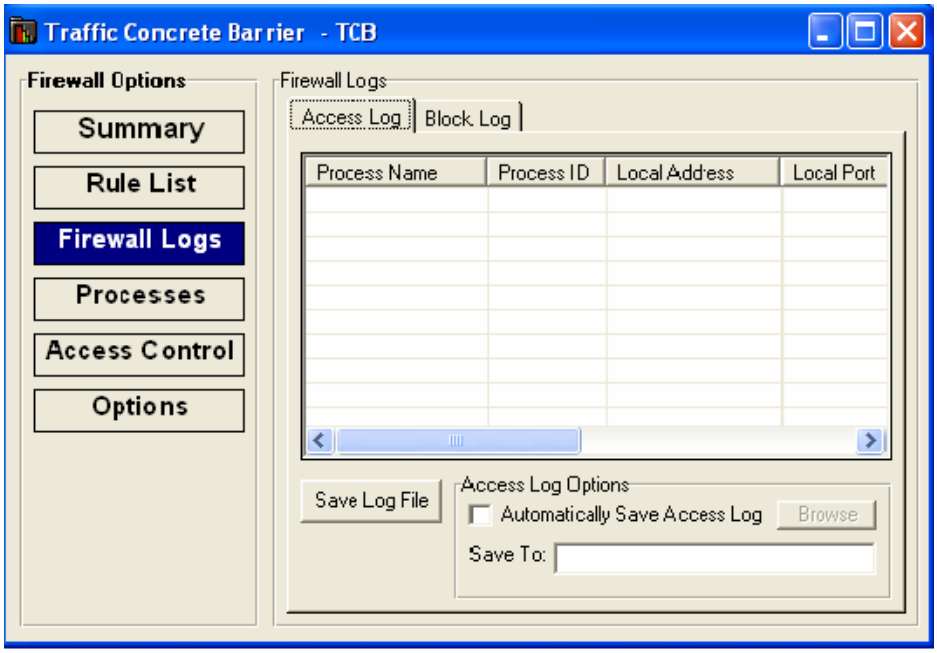

Figure 9- TCB Firewall Blocking Log

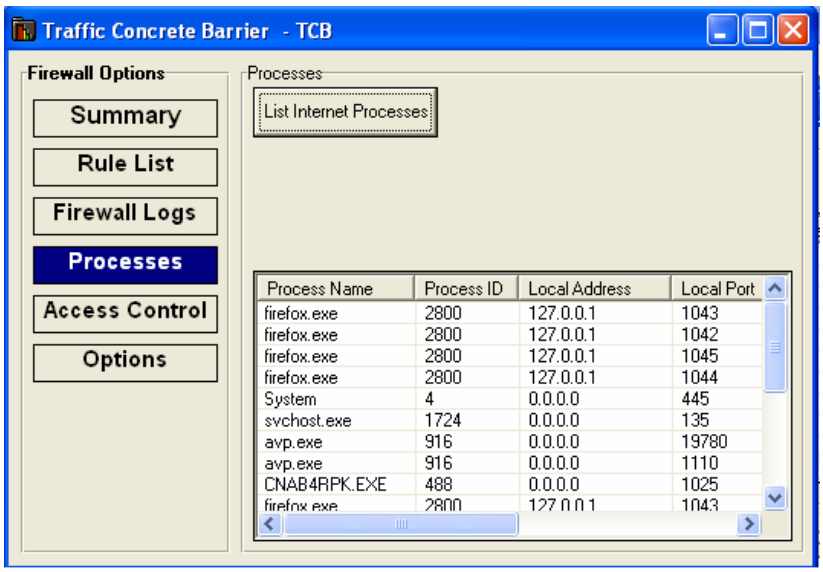

Figure 10- TCB Enumerating Process

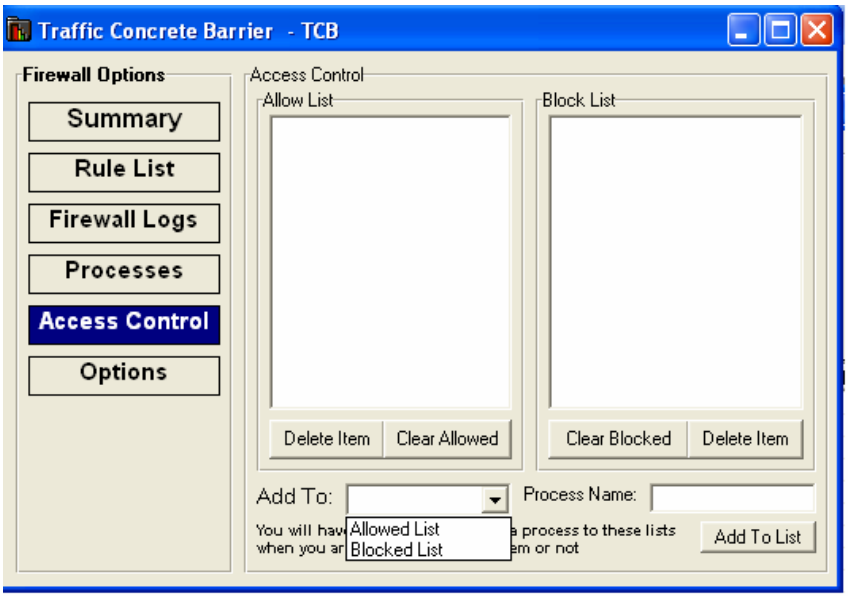

Figure 11- TCB Access Control List View

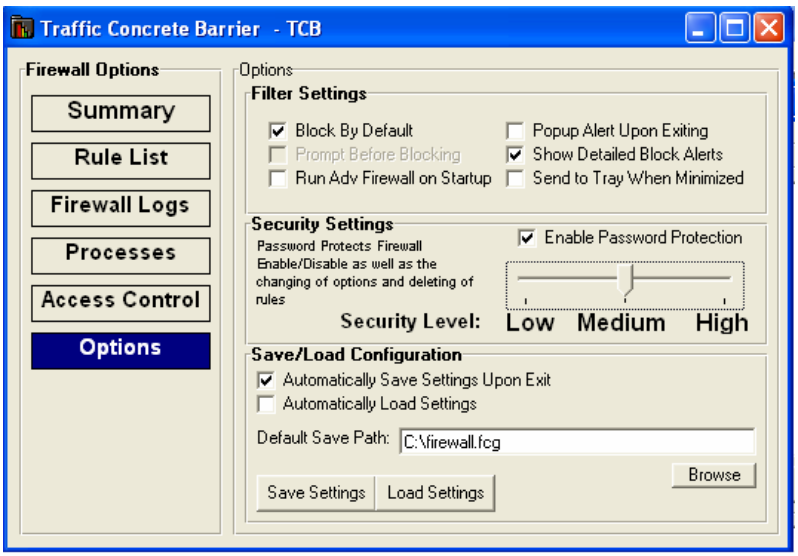

Figure 12- TCB Options /Security and Logging

Conclusions and Recommendations

1- Almost the time the attackers targeting the windows firewall and studying its weakness therefore it's more secure to use different firewall.

2- The interacting between the user and the firewall is the most important issue to perform the optimal security settings; therefore the efficient simplest GUI firewall is more secure Barrier.

3-Giving the ability for setting Blocking rules for incoming and outgoing traffic is vital to the computer security.

References

[1]: Wikipedia international Science online encyclopedia, en. wikipedia. org/ wiki/ Firewall

[2]: John.P.Wack, Keeping your site comfortable secure: An Introduction to Internet Firewalls, NIST Publication, 2005.

[3]: William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, Reading, 1994.

[4] Microsoft online Support – firewall configuration

www.microsoft.com/support/firewall.html.

الجدار الكونكريتي لتدفق البيانات المحلية والخارجية(TCB)

م.م علي عبد الحسين عبد الواحد

الملخص

يقدم هذا البحث برنامج الجدار الكونكريتي للبيانات المتدفقة في داخل النظام ومن خارجه (TCB) والذي يقوم بعمل خط دفاعي أولي لنظام الحاسبة وبالأخص نظام لويندوز والذي يقوم بمنع المتطفلين من البحث في الملفات المحلية أو من أي جهة خارجية.

الخاصية الرئيسية في هذا البرنامج هي عدم اعتماده أو استخدامه للجدار الناري الموجود في نظام الوندوز وهذا لكون الأخير قد اخترقت كل دفاعاته واستراتيجياته الدفاعية . يقوم برنامج الـTCB بحجب كل العمليات المشكوك فيها وحسب القوانين التي يضعها المستخدم في هذا البرنامج للعمليات المحلية منها والخارجية ، بالإضافة إلى حجب الـTps والمنافذ التي يحددها المستخدم وبصورة أوتوماتيكية تتم عملية الحجب بعد ما يتم فحص كل العمليات والمنافذ الموجودة حاليا في الحاسبة ساء على الصعيد المحلي أو الخارجي ، يتم حفظ القواعد الموضوعة من قبل المستخدم من خلال كلمة السر والتي وضعت من قبل المستخدم في البرنامج. برنامج الـTCB في هذا البحث يقوم بتوفير مستوى امني معقول لنظام الحاسبة على الصعيد المحلي والخارجي.