SYSTEM AND METHOD OF PREVENTING THE TRANSMISSION OF KNOWN AND UNKNOWN ELECTRONIC CONTENT TO AND FROM SERVERS OR WORKSTATIONS CONNECTED TO A COMMON NETWORK

FIELD OF THE INVENTION

The present invention generally relates to a method of preventing unauthorized access to Servers or Workstations connected to a common network medium such as the Internet. More specifically, the invention relates to a configuration of systems and methods for intercepting and removing undesirable content such as computer viruses from and to a common network.

DESCRIPTION OF BACKGROUND ART

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANET. The original aim was to create a network that would allow users of a research computer at one university to be able to "talk to" research computers at other universities. A side benefit of ARPANET's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

Today, the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP (for Transmission Control Protocol/Internet Protocol). Two recent adaptations of Internet technology, the intranet and the extranet, also make use of the TCP/IP protocol.

For many Internet users, electronic mail (e-mail) has practically replaced the Postal Service for short written transactions. Electronic mail is the most widely used application on the Net. You can also carry on live "conversations" with other computer users, using Internet Relay

Chat (IRC). More recently, Internet telephony hardware and software allows real-time voice conversations.

The most widely used part of the Internet is the World Wide Web (often abbreviated "WWW" or called "the Web"). Its outstanding feature is hypertext, a method of instant cross-referencing. In most Web sites, certain words or phrases appear in text of a different color than the rest; often this text is also underlined. When you select one of these words or phrases, you will be transferred to the site or page that is relevant to this word or phrase. Sometimes there are buttons, images, or portions of images that are "clickable." If you move the pointer over a spot on a Web site and the pointer changes into a hand, this indicates that you can click and be transferred to another site.

Using the Web, you have access to millions of pages of information. Web browsing is done with a Web browser, the most popular of which are Microsoft Internet Explorer and Netscape Navigator. The appearance of a particular Web site may vary slightly depending on the browser you use. Also, later versions of a particular browser are able to render more "bells and whistles" such as animation, virtual reality, sound, and music files, than earlier versions.

Today, the Internet being a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide, the security of the Internet is most important and systems like firewalls are used for security as shown in Figure 4.

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Basically, a firewall, working closely with a router (a logical device that routes the network information across networks, for example, routing network packets from private network to internet) program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access into the private network by the use of secure logon procedures and authentication certificates.

However the function of the firewall is limited in providing security at the operating system level only. At the Operating System level, the TCP/IP network protocol is monitored and filtered by the firewall. But various applications, for example, a Web Browser uses HTTP application protocol on top of TCP/IP network protocol to communicate with a Web Server. With TCP/IP being a transparent protocol, the firewall, since it filters at the Operating System level, will not be aware of HTTP protocol and will not check the contents represented in HTTP protocol and will authorize it immediately without checking.

U.S. Patent No. 6,499,107, has disclosed a method of identifying and stopping subsequent attacks based on attack signature left after the first attack. The method does not prevent the attacks in the first place, but based on a signature left, identifies them and prevents subsequent attacks. There is a need for a method that prevents the attacks in the first place itself.

U.S. Patent No. 6,496,935, has disclosed a method of accelerating the process of firewall filtering, but the filtering is carried out only at the operating system level, such as dealing with TCP/IP only. It does not filter the contents at the application level. There is a need for a method that does the filtering of application level protocols such as but not limited to HTTP at the application level.

Published US Patent Application No. 20030009689, has disclosed a method of relaying the message protocol from a network node inside a firewall protected network to the network outside the firewall by traversing the messaging protocol. The traversing is carried out to enable two-way communication between the network node inside the firewall and with the outside, which otherwise is difficult. But the method does not do the verification of contents of the messaging protocol for compliance, leaving room for the attacks to the application environment. There is a need for a method for interpreting the complete contents of the messaging protocol or the application network protocol and checking for its compliance with the protocol specification at IETF, thus preventing attacks to the application environment.

Examples of published documents that disclose technologies that deals only the operating system level verification but do not do application level packet filtering are:

i) IEEE published document part of 13th Annual Computer Security Applications Conference (ACSAC '97), December 08 - 12, 1997, San Diego, CA, Title: A reference model for firewall technology Internet URL: http://computer.org/proceedings/acsac/ 8274/82740133 abs.htm;

ii) IEEE published document part of 2000 IEEE Symposium on Security and Privacy (S&P 2000), May 14 - 17, 2000, Berkeley, California, p. 0177 Fang: A Firewall Analysis Engine, Title: A Firewall Analysis Engine, Internet URL: http://computer.org/proceedings/sp/ 0665/06650177abs.htm ;

iii) US Patent 5,832,208 discloses an anti-virus agent for use with databases and mail servers that principally detects and removes computer viruses located in attachments to e-mail messages. It does not prevent unknown viruses from attacking the systems in the network.

Such limitations are often used as an advantage by attackers to attack the servers by exploiting the flaws in various implementations of the Internet application protocol such as but not limited to HTTP (HyperText Transfer Protcol), FTP (File Transfer Program), SSH (Secure SHell), HTTPS (Secure-HypertText Transfer Protocol). The implementations of the application network protocol are done at the application level leaving all the application vulnerable to attacks.

The attacks include tasks such as but not limited to stealing private information, trade secrets and other important information with the computers in the private network or in the home.

SUMMARY OF THE INVENTION

To provide security for the communications between the applications, a new method of filtering is used in the invention. The method includes processing and interpreting of application network protocols used by the application across the network. It also prevents any information from reaching the application if it does not comply with the protocol specification.

The invention acts a proxy receiving information from the server, interpreting and verifying, then sending information to the client application like web browser and vise versa as shown in Figure 5.

The invention uses the protocol specification available at Internet Engineering Task Force (IETF) – www.ietf.org. The organization has various RFC (Request For Comments)

documents forming basis of various protocol implementations. Most implementations follow these specifications for compatibility reasons.

The protocol for which the invention provides security is as follows:

i) HTTP (HyperText Transfer Protocols);

ii) FTP (File Transfer Protocol);

iii) SSH (Secure SHell);

[0001] and other commonly used protocols.

[0002] Each and every protocol has guidelines defined by IETF and is used by the invention for compliance.

[0003] The invention also includes functions such as filtering based on content by preventing the unauthorized code from execution.

[0004] The invention will maintain a list of content that needs to be filtered and will automatically quarantine them. The list of "to be filtered content" can be maintained manually or can be automatically updated from the centralized server.

[0005] The contents can also be filtered based on the functions of the content such as modification of files, deleting of files and also creation of files. The functions are normally identified by the presence of a call to the operating system for the actions and scanning through each and every instruction in the content automatically identifies them.

[0006] In the invention the filtering is carried out by scanning through each and every network packet sent or received by the workstation or the server. The network packet is the minimal unit in the information transfer over the Internet.

[0007] The invention discloses a system for preventing the transmission of known and unknown electronic contents to and from servers or workstations connected to a common network comprising a means for interpreting contents of a messaging protocol or application network protocol; a means for checking compliance of the electronic contents with the messaging protocol specification or application network protocol specification; and a means for filtering the electronic content based on its functions. The system further includes a means for preventing attacks on the servers and/or workstations without knowing details of the attack. The means for interpreting contents of the messaging protocol or application network protocol comprises one or more servers, one or more workstations or combination thereof and intermediate verifier with protocol specification maintain therein. The means for interpreting contents of a messaging protocol or application network protocol comprises one or more

workstations and intermediate verifier with protocol specification maintain therein. The means for interpreting contents of a messaging protocol or application network protocol comprises one or more servers and intermediate verifier with protocol specification maintain therein.

[0008] The means for checking compliance of the electronic contents with the messaging protocol specification or application network protocol specification comprises one or more servers, one or more workstations or a combination thereof and an intermediate verifier with protocol specification maintained therein and wherein the one or more servers, the one or more workstations and the combination thereof and the intermediate verifier being the same as the one or more servers, the one or more workstations or combination thereof and the intermediate verifier stated earlier or are separately independent. The intermediate verifier checks compliance of the electronic contents between one or more servers or one or more workstations or combination thereof. The means for the filtering of the electronic content based on its function comprises a network of one or more servers and one or more workstations or combination thereof and at least one intermediate verifier functioning as a filter. The workstation is selected from one or more of the following Personal digital assistant (PDA); Personal computers; Mobile cellular telephone; or any apparatus with computing capability connected to a network.

[0009] The known and unknown electronic content is identified by one or more of the following pattern of binary codes within the electronic contents: Name of the electronic content such as name of file; Orientation and format of the electronic content such as plain text file, image file or data files; Function of the electronic content such as but not limited to erasure files without users knowledge or instruction, automatic sharing of files and corruption of files. A system wherein the patterns, names and orientation and format are used for filtering known content and the functions are used for filtering the unknown content. The unknown content, once identified to have a damaging function, has its name, pattern and orientation and format identified and stored in the database for further or future filtering. The identification and storage is done automatically.

[0010] The invention further discloses a method of preventing the transmission of known or unknown electronic content to and from servers or workstations or combination thereof connected to a common network comprising sending response information from one or more servers or one or more workstations or combination thereof to a designated recipient; verifying the response information by intermediate verifier before the information reaches the

designated recipient; relaying the verified information to the designated recipient and wherein the method of verifying includes the filtering of the known or unknown electronic content is based on its functions, patterns, names and orientation and formats of the electronic contents.

[0011] In another aspect the method of preventing the transmission of known or unknown electronic contents to and from servers or workstations or combination thereof connected to a common network comprises verifying of requested information by an intermediate verifier before information reaches a designated server or workstation or combination thereof wherein the method of verifying includes dispatching the verified information to a designated recipient and receiving request information by one or more servers or one or more workstations or combination thereof from one or more servers or one or more workstations. The method of verifying the information includes one or more of the following steps: checking the presence of known patterns in the electronic contents; checking the presence of known name of electronic contents such as name of file; checking orientation and format of the electronic contents such as plain text file, image file or data file; checking function of the electronic content such as but not limited to erasure files without users knowledge or instructions, automatic sharing of files and corruption of files. Yet in another aspect the method of preventing the transmission of known or unknown electronic contents to and from servers or workstations or combination thereof connected to a common network comprises sending response information from one or more server or one or more workstation or combination thereof to a designated recipient; verifying the response information by an intermediate verifier before information reaches the designated recipient; relaying the verified information to the designated recipient and wherein the method of verifying includes the interpretation of the messaging network protocol or application network protocol and checking its compliance with the application/network protocol specification available at IETF by the intermediate verifier programmed with such capabilities.

[0012] In another aspect the method of preventing the transmission of known or unknown electronic content to and from servers of workstations or combination thereof connected to a common network comprises verifying requested information by an intermediate verifier before information reaches the designated server or workstation or combination thereof; dispatching of verified information to a designated recipient and receiving requested information by one or more servers or one or more workstations or combination thereof from one or more servers or one or more workstations wherein the method of verifying includes the

interpretation of the messaging network protocol or application network protocol and checking its compliance with the application/network protocol specification available at IETF by the intermediate verifier programmed with such capabilities.

[0013] The invention further discloses a computer readable medium for verification for known or unknown electronic content transmitted between one or more servers or one or more workstations or combination thereof comprising program instructions for verifying the electronic content by checking the presence of known patterns in the electronic contents; checking the presence of known name of electronic contents such as name of file; checking orientation and format of the electronic contents such as plain text file, image file or data file; checking function of the electronic content such as but not limited to erasure files without users knowledge or instructions, automatic sharing of files and corruption of files and/or program instructions for checking it compliance with the application/network protocol specification available at the IETF programmed with such capabilities.

[0014] The program instructions are distributable through a common network such as the internet local area network or wide area network and are installed and/or executable in any computing device. The computer readable medium includes one or more CD roms, DVD, magnetic tapes, backup media or any media which is capable of storing computer program instructions. The media is connected to one or more servers, one or more workstations or combination thereof.

[0015] These and other aspects and advantages of the present invention will become apparent upon study of the following detailed descriptions and the accompanying diagram.

[0016] BRIEF DESCRIPTION OF DRAWINGS

[0017] The invention together with further advantages thereof, may be best understood by reference to the following description of preferred embodiments taken in conjunction with the accompanying drawings in which:

[0018] Figure 1 is a flow diagram of the process of proxying between the application server and application client and vice versa without any verification;

[0019] Figure 2 is a flow diagram of the process of filtering the unauthorized content;

[0020] Figure 3 is a flow diagram of the process of filtering of the application network protocols;

[0021] Figure 4 illustrates a prior art example of a network configuration incorporating a firewall; and

[0022] Figure 5 illustrates a network configuration incorporating a firewall between the internet and applicant client/operating system.

[0023] DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0024] In this description the term, 'common network' would include the Internet, Intranet, wide area network and other common networks.

[0025] Figure 1 is a flow diagram of the process of proxying between the application server and application client and vice versa without any verification. This is the process that takes place without any verification of information when configured to do so. The decision to not verify the contents is either done manually by the administrator or automatically by the system. The manual configuration is done in the facilities provided to administrators and is mainly used when the two network points are trusted and the information transferred between them is also trusted. The network point is either a Server serving information to the client or the Client receiving information from the Server.

[0026] The Server usually has an application program, also called "server programs" or "application server programs", that has instructions to send the information to the clients that connect to it and communicate based on the network protocol specification. An example of the server program could be a HTTP Server or Web Server. The client referred to herein is also the "application program" or "client program" that receives information from the server and optionally displays it to the user. An example of the client program could be a Web Browser.

[0027] In this process the invention acts as a proxy between the client and the server and relaying information between them. The information is referred to here as the "network packets." The network point or the point refers to the connection to a server or the client. The process starts with the waiting for information on a network point in step 101. This point could be a server or the client that sends the information.

[0028] The "waiting" referred to here can be a timed wait, that is, waiting for a specific number of seconds then checking for the information receipt, or event driven, that is, being notified by the Operating System on the information receipt. The waiting is indefinite unless interrupted by the users such as the people operating the personal computer and the

receipt of the information is checked in the step 102. If the information is not yet received, the process immediately continues at step 101.

[0029] But if the information is received, the process continues from step 103. In step 103, the program (part of the invention) connects to the other point as defined by the sending network point or a predefined location. The information about the other network point could be an IP address, a dot notation of the network computer location or DNS (Domain Naming System) name that will have to be mapped with an IP address or any other known computer location identification patterns. Upon connecting to the other point in the step 103, the process continues at step 104 where the information received at step 102 is sent to the other network point. After step 104, the process terminates.

[0030] Figure 2 is a flow diagram of the process of filtering the unauthorized content. This is the process that verifies information in the network packet before being sent to the other end. To accomplish this a list of unauthorized content will be maintained in the database. The database will have predefined list of the criteria of the unauthorized content and actions that the content is restricted to. The criterion in the database includes but not limited to the:

[0031] i) pattern - The patterns are a list of binary codes (zeroes and ones) grouped and are identified from the known damaging programs. These include programs that may spread viruses and may damage the files present in the personal computer.

[0032] ii) name - The name are a list of program names that are known to have damaging functions such as (but not limited to) erasing the information stored in the personal computer. The list may also contain sub-strings matching, parts of the full name given to the content.

[0033] iii) its orientation and format - This list contains the formats and the orientation of the content with damaging functions such as (but not limited to) erasing the information stored in the personal computer. The list also includes the formats of the unauthorized/restricted data.

[0034] iv) functions - This list contains the functions that are identified to be damaging such as (but not limited to) erasing files without user's instructions, automatically sharing important files, corrupting the files in the personal computer by scrambling them to a state from which the file cannot be retrieved to its original state.

[0035] The database will be maintained correctly and all necessary actions will be taken by the invention to keep the list with the latest information. The actions include but are

not limited to automatically updating information from a centralized repository and by automatically notifying the administrator about the availability of an update, if the update has to be done manually.

[0036] The functions are used for filtering unknown content whereas patterns, names and format are used for filtering known content. The unknown electronic content are identified by its functions and their patterns, names, format are automatically added to the database for further/future filtering.

[0037] The network point is either a Server serving information to the client or the Client receiving information from the Server. The Server usually has an application program, also called "server programs" or "application server programs", that has instructions to send the information to the clients that connect to it and communicate based on the network protocol specification. An example of the server program could be a HTTP Server or Web Server.

[0038] The client referred to herein is also the "application program" or "client program" that receives information from the server and optionally displays it to the user. An example of the client program could be a Web Browser. In this process the invention acts as a filtering mechanism between the client and the server and also relays only the authorized information between them. The information is referred to here as the "network packets."

[0039] The network point or the point refers to the connection to a server or the client, such as one or more workstations, one or more servers or any combination thereof. The process starts with the waiting for information on a network point in step 201. This point could be a server or the client that sends the information.

[0040] The "waiting" referred here can be a timed wait, that is, waiting for a specific number of seconds then checking for the information receipt, or event driven, that is, being notified by the Operating System on the information receipt.

[0041] The waiting is indefinite unless interrupted by the users such as the people operating the personal computer and the receipt of the information is checked in step 202. If the information is not yet received, the process immediately continues at step 201. But if the information is received, the process continues from step 203. In step 203, the program (part of the invention) connects to the other point as defined by the sending network point or a predefined location.

[0042] The information about the other network point could be an IP address, a dot notation of the network computer location or a DNS (Domain Naming System) name that will

have to be mapped with an IP address or any other known computer location identification patterns. Upon connecting to the other point in step 203, the process continues at step 204 where the information received at step 202 is checked with the list of unauthorized content. The list will include patterns, name, orientation and formats and functions. If the content matches with any of the criterion in lists, in step 205, the information will be blocked without sending to the other point. But if the content is authorized with its criteria not in the predefined lists, the information will be automatically sent to the other end in step 206 and the process terminates normally.

[0043] Figure 3 is a flow diagram of the process of filtering the application network protocol. This is, the process that verifies content in a communication between the application server and application client by checking compliance with the protocol specification as defined by IETF. For each and every application network protocol the contents will be checked for compliance with the exact protocol specification, that is, if the application uses HTTP 1.0 (HyperText Transfer Protocol) as their communication protocol, this process will check the communication contents with RFC 1945 defined by IETF. To accomplish this, the identification of the protocol used is carried out and is done by mapping the protocol with the port numbers used. A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User Datagram Protocol (commonly used subsystem of TCP/IP network protocol), a port number is a 16-bit integer that is put in the header appended to a message unit. This port number is passed logically between client and server transport layers and physically between the transport layer and the Internet Protocol layer and forwarded on.

[0044] For example, a request from a client to a server on the Internet may request a file be served from that host's File Transfer Protocol (FTP) server or process. In order to pass your request to the FTP process in the remote server, the Transmission Control Protocol (TCP) software layer in your computer identifies the port number of 21 (which by convention is associated with an FTP request) in the 16-bit port number integer that is appended to your request. At the server, the TCP layer will read the port number of 21 and forward your request to the FTP program at the server. Some services or processes have conventionally assigned permanent port numbers. These are known as well-known port numbers. In other cases, a port number is assigned temporarily (for the duration of the request and its completion) from a range of assigned port numbers. This is called an ephemeral port number.

[0045] From the assigned port numbers, the protocol that is being used is identified and the communication is checked with the respective specification defined by IETF. The network point is either a Server serving information to the client or the Client receiving information from the Server. The Server usually has an application program, also called "server programs" or "application server programs", that has instructions to send the information to the clients that connect to it and communicate based on the network protocol specification. An example of the server program could be a HTTP Server or Web Server

[0046] The client referred to herein is also the "application program" or "client program" that receives information from the server and optionally displays it to the user. An example of the client program could be a Web Browser. In this process the invention acts as a protocol filtering mechanism between the client and the server and also relays only the authorized information between them. The information is referred to as the "network packets." The network point or the point refers to the connection to a server or the client. The process starts with the waiting for information on a network point in step 301. This point could be a server or the client that sends the information.

[0047] The "waiting" referred here can be a timed wait, that is, waiting for a specific number of seconds then checking for the information receipt, or event driven, that is, being notified by the Operating System on the information receipt. The waiting is indefinite unless interrupted by the users such as the people operating the personal computer and the receipt of the information is checked in step 302. If the information is not yet received, the process immediately continues at step 301. But if the information is received, the process continues from step 303. In step 303, the program (part of the invention) connects to the other point as defined by the sending network point or a predefined location.

[0048] The information about the other network point could be an IP address, a dot notation of the network computer location or a DNS (Domain Naming System) name that will have to be mapped with an IP address or any other known computer location identification patterns. Upon connecting to the other point in the step 303, the process continues at step 304 where the information received at step 302 is checked for compliance with the specification defined by IETF for the protocol being used. If content does not comply with the specification, in step 305, the information will be blocked without sending to the other point. The compliance to the specification is verified by checking the Format of the data as required by the IETF specification; Process flow as required by the IETF specification. But if the content complies

with the specification the information will be automatically sent to the other end in step 306 and the process terminates normally.

[0049] Further, although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes, modifications, adaptations may be practiced within the scope of the claims. The described embodiments, the flow diagrams and architecture of the system should be taken as illustrative and not restrictive. The invention should not be limited to the details or parameters given herein, but should be defined by the following claims.

CLAIMS

1. A system for preventing the transmission of known and unknown electronic contents to and from servers or work stations connected to a common network comprising of:

means for interpreting contents of a messaging protocol or application network protocol;

means for checking compliance of the electronic contents with the messaging protocol specification or application network protocol specification; and

means for filtering the electronic content based upon one or more of the following:

pattern of binary codes within the electronic contents,

name of the electronic content,

orientation and format of the electronic content, or

function of the electronic content.

2. A system as claimed in Claim 1 further comprising of means for preventing attacks on the servers and/or work stations without knowing details of the attack.

3. A system as claimed in Claim 1, wherein the means for interpreting contents of a messaging protocol or application network protocol comprises of one or more servers, one or more work stations or combination thereof and intermediate verifier with protocol specification maintain therein.

4. A system as claimed in Claim 1, wherein the means for interpreting contents of a messaging protocol or application network protocol comprises of one or more work stations and intermediate verifier with protocol specification maintain therein.

5. A system as claimed in Claim 1, wherein the means for interpreting contents of a messaging protocol or application network protocol comprises of one or more servers and intermediate verifier with protocol specification maintain therein.

6. A system as claimed in Claim 1, wherein the means for checking compliance of the electronic contents with the messaging protocol specification or application network protocol specification comprises of one or more servers, one or more work stations or combination thereof and an intermediate verifier with protocol specification maintained herein and wherein the one or more servers, the one or more work stations and the combination thereof and the intermediate verifier is/are the same as the one or more servers, the one or more work stations or combination thereof and the intermediate verifier stated in Claim 3 or are separately independent.

7. A system as claimed in Claim 6, wherein the intermediate verifier checks compliance of the electronic contents between one or more servers or one or more work stations or combination thereof.

8. A system as claimed in Claim 1, wherein the means for the filtering the electronic content comprises of a network of one or more servers and one or more workstations or combination thereof and at least one intermediate verifier will functioning as a filter.

9. A system as claimed in Claim 1, wherein the work station is selected from one or more of the following: personal digital assistant (PDA); personal computers; mobile cellular telephone; or any apparatus with computing capability connected to a network.

10. A system as claimed in Claim 1, wherein the known and unknown electronic content is identified by one or more of the following:

pattern of binary codes within the electronic contents;

name of the electronic content such as name of file;

orientation and format of the electronic content such as plain text file, image file or data files;

function of the electronic content such as but not limited to erasure files without users knowledge or instruction, automatic sharing of files and corruption of files.

11. A system as claimed in Claims 1 and 10, wherein the patterns, names and orientation and format are used for filtering known content and the functions are used for filtering the unknown content.

12. A system as claimed in Claim 1, wherein the unknown content once identified to have a damaging function, its name, pattern and orientation and format will be identified and stored in the database for further or future filtering.

13. A system as claimed in Claim 12 wherein the identification and storage is done automatically.

14. A method of preventing the transmission of known or unknown electronic content to and from servers or work stations or combination thereof connected to a common network comprising of:

sending response information from one or more servers or one or more work stations or combination thereof to a designated recipient;

verifying the response information by intermediate verifier before the information reaches designated recipient;

relaying the verified information to the designated recipient and wherein the method of verifying includes the filtering of the known or unknown electronic content is based on its functions, patterns, names and orientation and formats of the electronic contents.

15. A method of preventing the transmission of known or unknown electronic contents to and from servers or work stations or combination thereof connected to a common network comprising of:

verifying of requested information by an intermediate verifier before information reaches a designated server or work station or combination thereof;

despatching the verified information to a designated recipient; and

receiving request information by one or more servers or one or more work stations or combination thereof from one or more servers or one or more work stations.

16. A method as claimed in Claims 14 and 15, wherein the method of verifying the information includes one or more of the following steps:

checking the presence of known patterns in the electronic contents;

checking the presence of known name of electronic contents such as name of file;

checking orientation and format of the electronic contents such as plain text file, image file or data file;

checking function of the electronic content such as but not limited to erasure files without users knowledge or instructions, automatic sharing of files and corruption of files.

17. A method of preventing the transmission of known or unknown electronic contents to and from servers or work stations or combination thereof connected to a common network comprising of:

sending response information from one or more server or one or more work station or combination thereof to a designated recipient;

verifying the response information by an intermediate verifier before information reaches the designated recipient;

relaying the verified information to the designated recipient and wherein the method of verifying includes the interpretation of the messaging network protocol or application network protocol and checking its compliance with the application/network protocol specification available at IETF by the intermediate verifier programmed with such capabilities.

18. A method of preventing the transmission of known or unknown electronic content to and from servers or work stations or combination thereof connected to a common network comprising of:

verifying requested information by an intermediate verifier before information reaches the designated server or work station or combination thereof;

despatching of verified information to a designated recipient; and

receiving requested information by one or more servers or one or more work stations or combination thereof from one or more servers or one or more work stations

wherein the method of verifying includes the interpretation of the messaging network protocol or application network protocol and checking its compliance with the application/network protocol specification available at IETF by the intermediate verifier programmed with such capabilities.

19. A computer readable medium for verification for known or unknown electronic content transmitted between one or more servers or one or more work stations or combination thereof comprising of program instructions for verifying the electronic content by:

checking the presence of known patterns in the electronic contents;

checking the presence of known name of the electronic contents such as name of file;

checking orientation and format of the electronic contents such as plain text file, image file or data file;

checking function of the electronic content such as but not limited to erasure files without users knowledge or instructions, automatic sharing of files and corruption of files and/or program instructions for checking its compliance with the application/network protocol specification available at the IETF programmed with such capabilities.

20. The program instruction as claimed in Claim 19 distributable through a common network such as the internet local area network or wide area network.

21. The program instruction as claimed in Claim 19 which is installed and/or executable in any computing device.

22. Computer readable medium as claimed in Claim 19, wherein the medium includes one or more CD ROM, DVD, magnetic tapes, backup media or any media which is capable of storing computer program instructions.

23. Computer readable medium as claimed in Claim 19, wherein the media is connected to one or more servers, one or more work stations or combination thereof.