(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
14 December 2006 (14.12.2006)

(10) International Publication Number
WO 2006/131124 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/DK2006/000327

(22) International Filing Date: 9 June 2006 (09.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
pa 2005 00856 10 June 2005 (10.06.2005) DK
PA 2005 01495 28 October 2005 (28.10.2005) DK

(71) Applicant *(for all designated States except US)*: **GATESWEEPER SOLUTIONS INC.** [PA/PA]; The Belvedere Park Bld. Apt.9, 1st Street, Coco Del Mar, San Francisco, Panama City (PA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **THOMASSEN, Rene** [DK/DK]; Pedersmindevej 7, Kastbjerg, DK-8970 Havndal (DK).

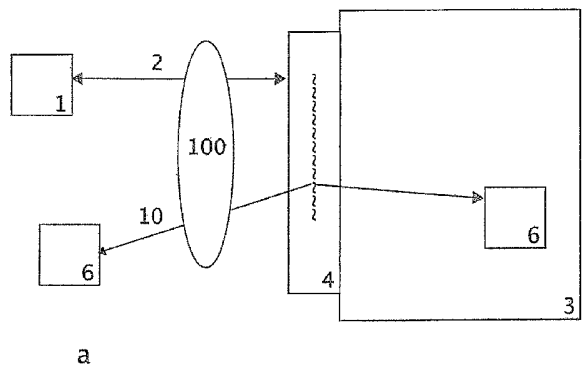
(74) Agent: **PATRADE A/S**; Fredens Torv 3A, DK-8000 Aarhus C (DK).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

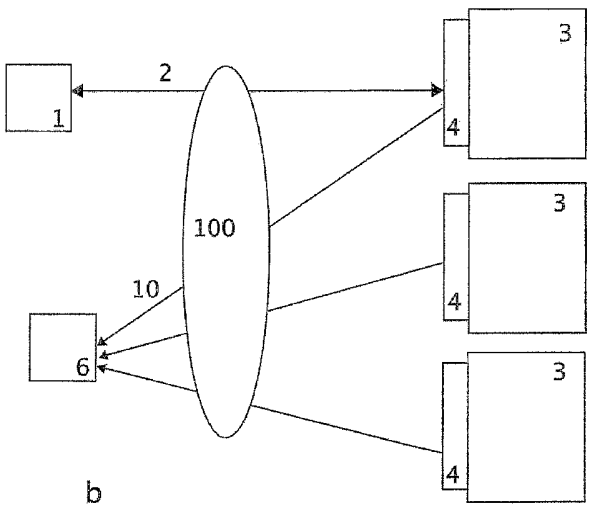
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title:** ANTI-HACKER SYSTEM WITH HONEY POT



a



b

(57) **Abstract:** Anti-hacker system for counteracting a hacker attack on a computer system, wherein the anti-hacker system comprises a computer system with a firewall configured upon a recognised attack on the computer system to forward the attack into a honey pot system without a for the hacker noticeable change of IP address. The honey pot system is located outside the computer system with the firewall. The system may comprise a number of ports that are open to hacker attack and the ports are protected by a number of built-in "Bouncers", which works as a transparent proxy server, configured to forward the attack into the honey pot.

WO 2006/131124 A1

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Anti-hacker system with honey pot

FIELD OF THE INVENTION

The present invention relates to an anti-hacker system for counteracting a hacker attack on a computer system, wherein the anti-hacker system comprises a computer system with a firewall configured upon a recognised attack on the computer system to forward the attack into a honey pot system without a for the hacker noticeable change of IP address.

BACKGROUND OF THE INVENTION

With the growing and constant threat of unauthorized intrusion, computer systems need the protection of security software to help them keep running safely while eliminating the source of break ins. In the home, these invasions can be annoying at the best and extremely costly at worst. For businesses and organizations, security breaches can result in compromised information, lost revenue and hours of work and expenses to repair or replace programs and systems.

Firewalls are a form of security software and hardware that attempt to provide protection to computer systems by disallowing traffic from the internet or from another computer on a network when it does not confirm to a specific set of guidelines or filters. They protect from intentional hostile intrusion that might compromise sensitive data or result in a corruption of data or denial of service.

Firewalls are an essential first line of defense for protecting computer systems. Anyone who has a computer that is connected to the Internet needs firewall protection.

But, not all firewalls are created equal. Up until now, the typical firewalls on the market have acted as barriers between computers on a network, whether that is a business network or the World Wide Web. Without firewalls, intruders on a network would be able to destroy, tamper with or gain access to the files on many computers.

The ability of an anti-hacker vendor to identify new methods of hacking and to develop firewalls to prevent the hackers and crackers from gaining access to user machines is fundamental to the effectiveness of their solutions. Unfortunately, the typical

firewall on the market today only prevents break-ins. Once denied access, the hacker will just continue on to the next inadequate protected computer where he might be successful in his destructive and criminal behavior. Therefore, a number of systems have been developed counteracting hacker attacks.

A computer system is disclosed in European patent application EP 1 218 822 by Roesch et al., where the disclosed computer system comprises a real network and a virtual network. An attempt of use of the virtual network is regarded as a hacker attack and information about the hacker is gathered in order to update the firewall of the real network in order to prevent attack in this network

In order to otherwise reduce the damage of hacker attack on a computer system, there has been provided systems, as illustrated in FIG. 1, where the hacker 2 attack is redirected 10 into a second system 6, which has the purpose to give the hacker 1 the impression to have entered the computer system 3 through a firewall 4, but which in reality is a simulated system where damage is of no concern.

Such a system is called a "honey pot" due to the association with baits used to catch insects. Likewise, the honey pot is used to catch and keep the hacker in an environment, which the hacker experiences as desired goal. During presence of the hacker attack in the honey pot, the hacker may in some instances be traced in order to find the address from which the sending occurs.

However, the described system has the disadvantage that the IP address of the honey pot is different than the IP address towards which the attack was directed. The experienced and alert hacker would immediately recognize this and terminate the attack or try a new attack in a different way.

Overcoming this problem, a computer system with a honey pot is disclosed in US patent No. 5,884,025 by Baehr et al., where a recognized attack is redirected into a honey pot without a for the hacker noticeable change of IP address.

In line with more efficient firewalls and advanced security systems, hackers get more sophisticated as well. This puts a steady demand on development of security routines. The disclosure in US 5,884,025 is a system that is used within private computer sys-

tem networks making the system expensive, costing in the price range from $20,000 to $500,000 depending on the size of corporation. Therefore, it is normally only seen in bigger corporations. It requires an IT-Department and maintenance service. In such a system, there are at least three physical computers, of which two are used for the security system (IDP/Firewall and honey pot). In reality there would probably be minimum 5-10 or maybe up to hundreds of computers protected behind a system like this.

It would be desirable to provide systems with equally high security but at lower costs.

DESCRIPTION / SUMMARY OF THE INVENTION

It is therefore the purpose of the invention to provide a low cost system that may be used to reduce the possibilities of damage in personal computer by unauthorized intruders.

This purpose is achieved by an anti-hacker system for counteracting a hacker attack on a computer system, wherein the anti-hacker system comprises a computer system with a firewall configured upon an attempted attack on the computer system to forward the attack into a honey pot without a for the hacker noticeable change of IP address, and wherein the honey pot is located outside the computer system with the firewall.

By locating the honey pot outside the computer system with the firewall – or likewise, outside a private network system – there is a possibility for many private customers to use firewalls that share the same single honey pot. This provides a system at much lower costs that the above mentioned system, where the honey pot is provided inside the computer system with the firewall.

In a preferred solution, the system comprises a public digital data network, for example the Internet, a computer system connected to the public network, and a honey pot system connected to the public network for communication between the computer system and the honey pot system only through the public network system. In this case, the honey pot may be part of a commercial system to which customers with personal computers or other computer systems may subscribe. In the case of the network being the Internet, the honey pot may be available for a large number of users independent of geographical distance.

A good solution at low cost is a firewall that is implemented as a software program in the computer system. Such software programs are easily distributed in large numbers, for example via the Internet for download on computer systems, such as a personal computer.

A practical embodiment is achieved by configuring the system with one or more dedicated computer ports through which entry is possible through the firewall, but only with a subsequent redirection into a honey pot. The system is configured such that the hacker experiences an apparent entry into the system without noticeable change of IP address. The redirection is achieved through a unique built-in, rule based bouncer software program. The unique bouncers work similarly to a transparent proxy server behind the apparently open port, which makes any IP address change invisible to the hacker. The rule based aspect of the bouncer allows and easy configuration.

In the following, the term "honey pot port" is used for a port that leads into a Honey-Pot. The term "true port" is used for ports in the computer system that lead into the true computer system, which means not into a honey pot. The term "true system" is used for the computer system into which no access is desired by hackers.

During a hacker attack, the attack is lead through certain, for the hacker apparently open ports in the firewall. Once the attack has gone through the ports, the hacker has the impression that the computer system has been entered. However, the attack is invisibly to the attacker redirected by the unique bouncers to another location on the internet and into the honey pot. The hacker experiences the actions inside the honeypot as if the system responses to the instructions from the hacker. However, once inside the honey pot, no damage can occur to the system because the honey pot is located another place on the internet and not used for anything else than keeping the hacker busy and collecting information about the hackers activities. In this connection, it should be emphasized that according to prior art, no hacker identification routines are yet commercially available for personal computers.

In order to have a high probability for leading possible hacker attacks into honey pots, certain ports may be used for leading the hacker attack. Typically, there are 65 thou-

sands of possible ports and a few of them have dedicated functions under normal use, such as ports number 20 (FTP Data), 21 (FTP), 22 (SSH), 23 (TELNET), 25 (SMTP, mail server), 80 (HTTP, web server), 110 (POP3, mail account). Due to the fact that these ports are typically the only ports that are open for public access because of their dedicated functions, such ports have a high likelihood to be object for attacks.

Typically, a hacker scans a number of IP addresses for open ports. The scanning is typically performed systematically on all subsequent ports. If the hacker normally finds an open, dedicated port, it indicates the type of server, the attack is directed towards. For example, if the open port is port number 25, the hacker has an indication that the attacked server is a mail server with the corresponding security system typical for mail serers. The hacker may in this case use certain developed tools for entering the computer through the mail server security system, for example the creation of a buffer overflow causing the execution of computer commands during emptying of the buffer.

The invention simulates a vulnerable computer system, by apparently having the following 7 ports open; 20 (FTP Data), 21 (FTP), 22 (SSH), 23 (TELNET), 25 (SMTP, mail server), 80 (HTTP, web server), 110 (POP3, mail account). When the hacker performs a random port scan, these ports will look open. This will attract potential hackers. However each of these ports are protected by the unique built-in "Bouncers".

In that way, a potential hacker would get past the physical firewall, but then the advanced bouncer software program, which works as a transparent proxy server, would redirect the potential hacker to the honey pot. One is then able to collect the electronic evidence used to apprehend the potential hacker.

The choice of ports to be open for hacker attack and be protected by the "bouncers" can be chosen by the programmer dealing with the configuration of the system.

In order to reduce hacker attacks in general, the honey pot may optionally be configured to gather information about the attack. The information is forwarded to a central server in order to keep track of attacks in general and of specific types of attacks. The information is used to upgrade the firewall software. Also, once caught in the honey pot, information about the attack can be used to trace the hacker address for with help

by the police to prevent further actions from the hacker. For example, if a hacker attack has been found, the open ports may be blocked by the firewall for a certain time for these specific IP addresses. In connection with a web port or an e-mail port, the firewall may be configured to let the port be open to any IP address in general but to check the entering IP addresses, whether the entering address is equal to one of those that have been associated with a hacker attack.

Having a large number of open ports is also advantageous, because this typically attracts a large number of hackers. On one hand, this increases the amount of information about hacker attacks in general and may give information about certain hacker strategies. In addition, while hackers are working in honey pots, they are busy and cannot make real damage.

For hackers that are frequently in honey pots, attacks get increasingly less interesting. Due to the large amount of open ports connected to honey pots, the hacker cannot easily experience, whether a port is a port into the true system or whether it leads into a honey pot. In a first strategy, the honey pot ports may be made easy to enter in order for the port to attract most hackers, as most hackers choose the easiest ways into the true system. In contrast, open ports into the true system may be secured by the typical security system for this type of ports. In addition, some ports are only open to certain IP addresses.

However, clever hackers may after some honey pot experience search for ports that are not so easy to access or ports, where it seems to be somewhat difficult to get further into the true system. Therefore, in a second strategy, the honey pot ports may be camouflaged by covering the entry with an apparent – but not true – security system. This security system is configured to give the hacker a certain resistance, such that the hacker believes that this is an entrance to the true computer system and not just another easy access to a honey pot. However, also these ports lead to a honey pot after apparent victory of the hacker attack over this apparent security system.

By configuring the computer system to comprise easy accessible honey pot ports, difficult accessible honey pot ports, and difficult accessible ports into true computer system, the probability for trapping of hackers in honey pots is increased, because in this case, the likelihood for being trapped in a honey pot is high not only for inexperienced

hackers that go for easy entrance but also for experienced hackers that aim to enter the system only if there is a certain resistance.

A simple method in a honey pot to keep the hacker busy is to repeatedly answer attacks with standard phrases that increase the effort of the hacker to get further into the system, such as a standard phrase expressing that the submitted commend is not understood by the system or a phrase expressing that an entrance is accepted. Meanwhile the honey pot may collect information about the hacker attack.

The security system according to the invention may be additionally secured in a further embodiment. In this case, the computer system analyses the request for entering the ports. In case that the request is sent to a number of ports subsequently, which indicates a port scanning by a hacker, certain ports, namely the access ports to the true system, may be closed for this specific IP address or closed in general for a short while in order to prevent the hacker to enter through these specific ports.

Additionally, the computer system according to the invention may be configured to check for attempts from hackers to create buffer overflows by a large number of requests within short time spans. Also in this case, true access ports may be closed for a certain time for the specific IP address or in general in order to keep the system safe from hacker attacks that would destabilize the system.

The information that is collected in the honey pots may, as mentioned above, be used later for additional security. For example, it may occur that certain hacker attacks use certain programmed attack codes in order to enter computer systems. Such code blocks may be distributed to various associated computer systems using a safety system according to the invention, where the safety system is configured to generally check access requests, whether the requests do contain such blocks of code. If a request can be recognized as containing this kind of code blocks, certain true ports may be closed for a certain while in order to protect the system against hacker attacks.

The security system according to the invention has an increased performance if it is installed on an increasingly number of computer systems. This is so, because each computer with the invention installed becomes an advanced honey pot. The honey pot system is able to record both known methods of hacking as well as unknown methods

of hacking. Once recorded by the honey pot, an update of all firewall software programs can be performed to achieve more effective guard against future hacker attempts.

SHORT DESCRIPTION OF THE DRAWINGS

The invention will be explained in more detail with reference to the drawing, where

FIG. 1 illustrates the prior art principle of a redirection of a hacker attack into a honey pot,

FIG. 2 illustrates the principle of the invention,

FIG. 3 shows a flow diagram of the principle,

FIG. 4 illustrates the system according to the invention in greater detail

FIG. 5 illustrates the Rules menu of the toolbox,

FIG. 6 illustrates the LogMonitor menu of the toolbox,

FIG. 7 illustrates the InformationCenter menu of the toolbox,

FIG. 8 illustrates the HoneySet menu of the toolbox,

FIG. 9 illustrates the Statistics menu of the toolbox.

DETAILED DESCRIPTION / PREFERRED EMBODIMENT

FIG. 2a and b illustrates the principle of the invention. A hacker/intruder 1 may attack 2 a computer system 3 in order to enter through the firewall 4. The firewall may be a hardware firewall but, preferably, is a software program implementet in the computer system 3. The firewall 4 is programmed to register the attack 2, which initiates a number of computer routines. The attack is not redirected, which would imply a new IP address, but is forwarded 10 instead into a honey pot 6 outside the computer system 3 with the firewall 4, for example by a transparent proxy server implemented in the firewall 4, such that the hacker would not experience any redirection to a different IP address. Thus, the hacker may use his efforts in a system, namely the honey pot, where

damage is of no concern to the rest of the network. As illustrated in FIG. 2b, the attack may reach the computer system 3 through a public network system 100, for example the Internet. The attack may then be forwarded to a honey pot 6. The honey pot 6 may serve several computer systems with firewalls, all connected to the public network, where the communication to the honey pot 6 from the computer systems 3 with the firewalls 4 only through the public network.

For example, the attack 2 from the hacker 1 may be allowed to enter through one of the ports 5 of the firewall, which is illustrated in more detail in FIG. 4, but the attack is not allowed to enter the system 3 as such, where damage may occur. Instead, the attack 2 is forwarded 10 into a honey pot 6 located outside the computer system 3 with the firewall 4, for example at another place on the internet 100. This can be achieved by the unique "Bouncer" software programs 7 behind the firewall. In any case, response 8 from the honey pot is received and forwarded 9 to the hacker from the IP address associated with the attacked firewall 4. This way, the security system with the firewall 4 acts as a transparent proxy server 7 during the attack such that the hacker does not experience any indication of the fact that the attack has been redirected into a honey pot 6.

In order for the system according to the invention to operate, a number of routines from known software programs may be utilized. This serves as example only and is not limiting for the principle of the invention. In connection with the firewall, routines from winsock.dll, such as Hooking, Send(), receive(), and connect() are used, where data packages are parsed/redirected before entering the stack where overflow may occur. If the packages are not allowed, they typically are rejected. However, in connection with the honey pot, the packages may be forwarded in a bounced connection to a different IP without change of the packages and without noticeable change of IP due to the transparent proxy behind the firewall. This way, the traffic is forwarded to a different server (honey pot), where all technical evidence is accumulated.

The traffic may run the protocol TCPIP TCP and UDP supported by the firewall, or tsl/ssl may be used in the case of encryption. The forwarding/redirection happens before the traffic gets access to the tcp/udb stack of the computer system such that it is

not possible for the hacker at achieve a stack overflow which would destabilize the system for access thereto.

FIG. 3 is a flow diagram of the principle of how the rules in the invention work.

In FIG. 5, part of the user interface of the system according to the invention is illustrated. The program implementing the invention is for simplicity called GateSweeper and comprises a user interface with a Toolbox having different tools. One of the tool menus, namely the Rules Menu 11 governs setting of the rules for the security system. In the first column 12, certain IP addresses may be set for allowance or denial of requests from computers with those IP numbers. The allowance or denial through certain pre-chosen ports of the system is set in the second column 13. In addition, the port type may be pre-selected (for example TCP/UDP, FTP, SSH, Mail, etc.) in the third column 14 and the degree of permission in column four 15. For example, entrance may be denied for all IP numbers, such that the mentioned ports are entirely closed. Alternatively, certain selected ports may be completely open to certain pre-chosen IP numbers, or even open to requests from any IP number. The configuration of the of the security system by rules is very easy for the user to perform and gives a good overview, making the system according to the invention very user friendly.

Furthermore, as illustrated in the lower part of the menu, certain programs may be selected in the Application path column 16 with corresponding settings (generally allowed or generally denied) in the Permission column 17. Changes to these settings/rules to the IP Add column 12 or the Application Path column 16 can be made by adding or deleting rules, which is initiated by activating the corresponding buttons 18, 19 in the bottom part.

In addition, there are a number of pre-set rules handling requests for entrance to the system in the lower right part 20 of the Rules Menu, where the term OPEN refers to the fact that the system is open. The term STANDARD refers to the setting, where allow rules and deny rules are obeyed and the system uses the predefined rules. The term PARANOID is used as a pre-setting, where the system is generally closed for traffic.

In FIG. 6, a second part of the user interface is illustrated, namely the Log Monitor. The Log Monitor shows any traffic into and out of the computer.

In FIG. 7, the Information Center menu of the system is illustrated. It contains information about attack attempts that have been redirected into the honey pot. The information from the honey pot and from the Information Center is forwarded to a central server, where statistics are performed concerning the attacks, and where studies are made concerning the methods used by different hackers. The central server system also is responsible for the evaluation of the technical evidence concerning the attack as gathered in the honey pot and responsible for the update and reconfiguration of firewalls in order to prevent further successful attempts for intrusion.

In FIG. 8, the menu HoneySet for the settings of the "Bouncers" is illustrated. When one or more of the 7 ports listed below are marked, the system will look vulnerable to a potential hacker. This means each port will look OPEN, but in reality it is protected by the unique "Bouncer" technology built-in the personal computer firewall software.

- ☐ 20 (FTP Data)
- ☐ 21 (FTP)
- ☐ 22 (SSH)
- ☐ 23 (TELNET)
- ☐ 25 (SMTP, mail server)
- ☐ 80 (HTTP, web server)
- ☐ 110 (POP3, mail account)

If a hacker tries to attack one or more of the above listed ports and the "Bouncer" is activated the hacker will be invisibly to the hacker redirected to the honey pot.

If one or more ports are left unmarked the port will be closed by the Firewall. Any attempt to hack will be blocked.

In FIG. 9, a server status is illustrated, showing the number of hacker attacks in different countries. The number of attacks illustrated depends on the actual attack frequency and on the number of computers that are using the system according to the invention.

The invention may in a further embodiment be used as a sniffing system for attack methods for an immediate updating of firewalls. For example, while the hacker attack resides in the honey pot, information is collected about the attack, for example: How the attack is performed? Which are the points of attack? Where are weaknesses expected? This information may be collected in a central database, for example in a world-wide anti-hacker system, and be used to upgrade the firewalls associated with this anti-hacker system. In principle, a scenario as the following may occur: A hacker tries to enter a computer system through a firewall and the attack is forwarded into a honey pot. Information is collected in the honey pot and via a computer network, for example the Internet, transmitted to a central server. The central server initiates an immediate update of the firewalls of all users/subscribers of the system. The update may be performed soon after the hacker has been using his efforts in the honey pot. Once the hacker exits the honey pot, the same method of attack or the same IP address would after a few minutes be useless on all the firewalls associated with this central server system.

CLAIMS

1. Anti-hacker system for counteracting a hacker attack on a computer system, wherein the anti-hacker system comprises a computer system with a firewall configured upon a recognised attack on the computer system to forward the attack into a honey pot system without a for the hacker noticeable change of IP address, characterised in that the honey pot system is located outside the computer system with the firewall.

2. Anti-hacker system according to claim 1, wherein the system comprises a public digital data network, a computer system connected to the public network, and a honey pot system connected to the public network for communication between the computer system and the honey pot system only through the public network system.

3. Anti hacker system according to claim 1, wherein the system comprises a public digital data network, a number of mutually independent computer systems with firewalls connected to the public network, and a honey pot system connected to the public network for communication between the honey pot system and each computer system of the number of computer systems only through the public network system.

4. Anti-hacker system according to claim 2 or 3, wherein the public network system is the Internet

5. Anti-hacker system according to any preceding claim, wherein the firewall is implemented as a software program in the computer system.

6. Anti-hacker system according to any preceding claim, wherein the computer system is a personal computer.

7. Anti-hacker system according to any preceding claim, wherein the firewall of the computer system comprises a number of data ports that are configured to be open to hacker attack and protected by a built-in, rule based bouncer technology functioning as a transparent proxy-server and being configured for forwarding the attack from the open port into the honey pot of the honey pot system.

8. Anti-hacker system according to claim 7, wherein the firewall of the computer system comprises a number of data ports that are configured to be open to hacker attack only to a certain degree in order to give the hacker a certain resistance before entrance through a port.

9. Anti-hacker system according to any preceding claim, wherein the firewall is configured to check for apparent systematic scanning for open ports, and configured to close preselected ports upon recognition of this systematic scanning.

10. Anti-hacker system according to claim 9, wherein the preselected ports are closed for a predetermined time upon recognition of this systematic scanning.

11. Anti-hacker system according to any preceding claim, wherein the firewall is configured to check, whether an IP address in connection with a data request earlier has been recognised as associated with a hacker attack, and in the affirmative closing pre-selected ports for access in relation to the IP address.

12. Anti-hacker system according to any preceding claim, wherein the firewall is configured to check for attempts from potential hackers to create buffer overflows by a large number of requests within short time spans.

13. Anti-hacker system according to any preceding claim 12, wherein in the affirmative, access ports that are not related to a honey pot are closed for a predetermined time for the specific IP address.

14. Anti-hacker system according to any preceding claim 12, wherein in the affirmative all access ports are closed for a predetermined time.

15. Anti-hacker system according to any preceding claim, wherein the honey pot system is configured for collecting information in the honey pot about the attack and configured to forward the information to a central server.

16. Anti-hacker system according to claim 15, wherein the central server is configured upon receipt of this information to forward commands to associated computer systems for upgrading their firewalls in dependence of the information.

17. Anti-hacker system according to claim 16, wherein the system is configured to check in the collected information from the honey pot for blocks of programming code that appear to be hacker attack tools, and is configured for selecting these code blocks for use in the upgrade of firewalls.

18. Anti-hacker system according to claim 16, wherein the system is configured to check in the collected information from the honey pot for blocks of programming code that appear to be hacker attack tools, and is configured for closing certain ports for a certain while in order to protect the system against hacker attacks.

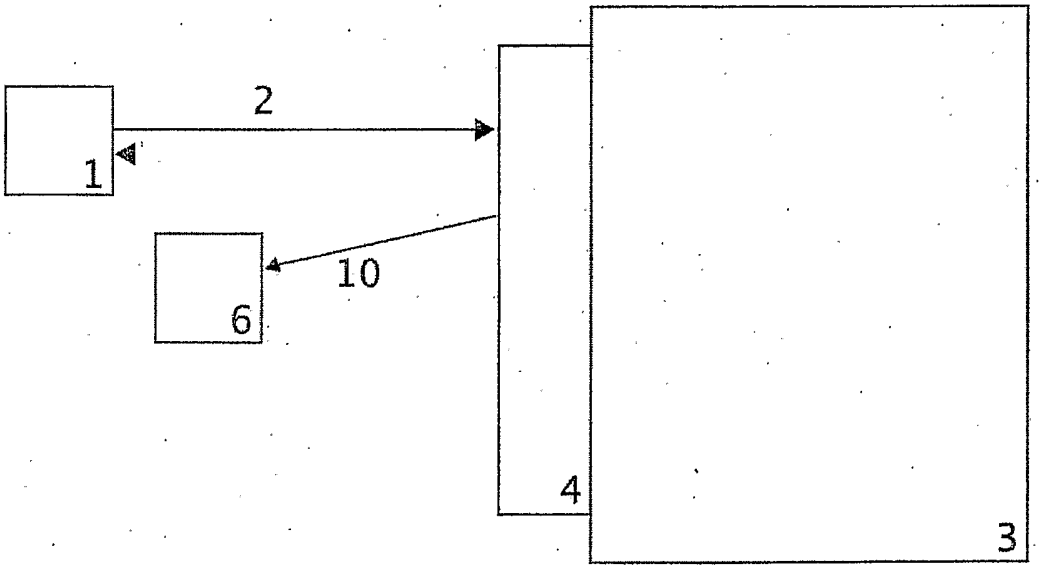


FIG. 1

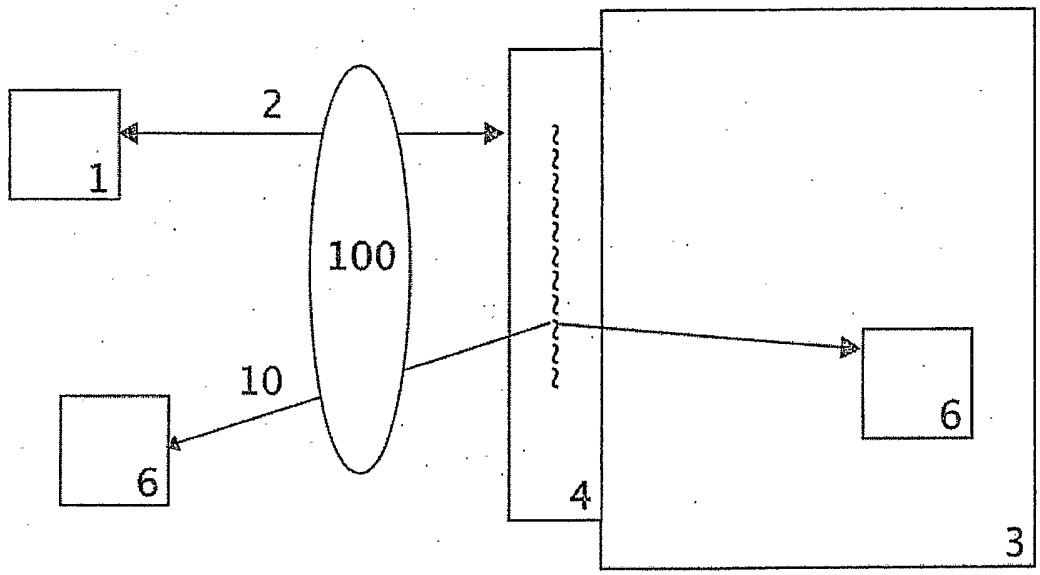


FIG. 2a

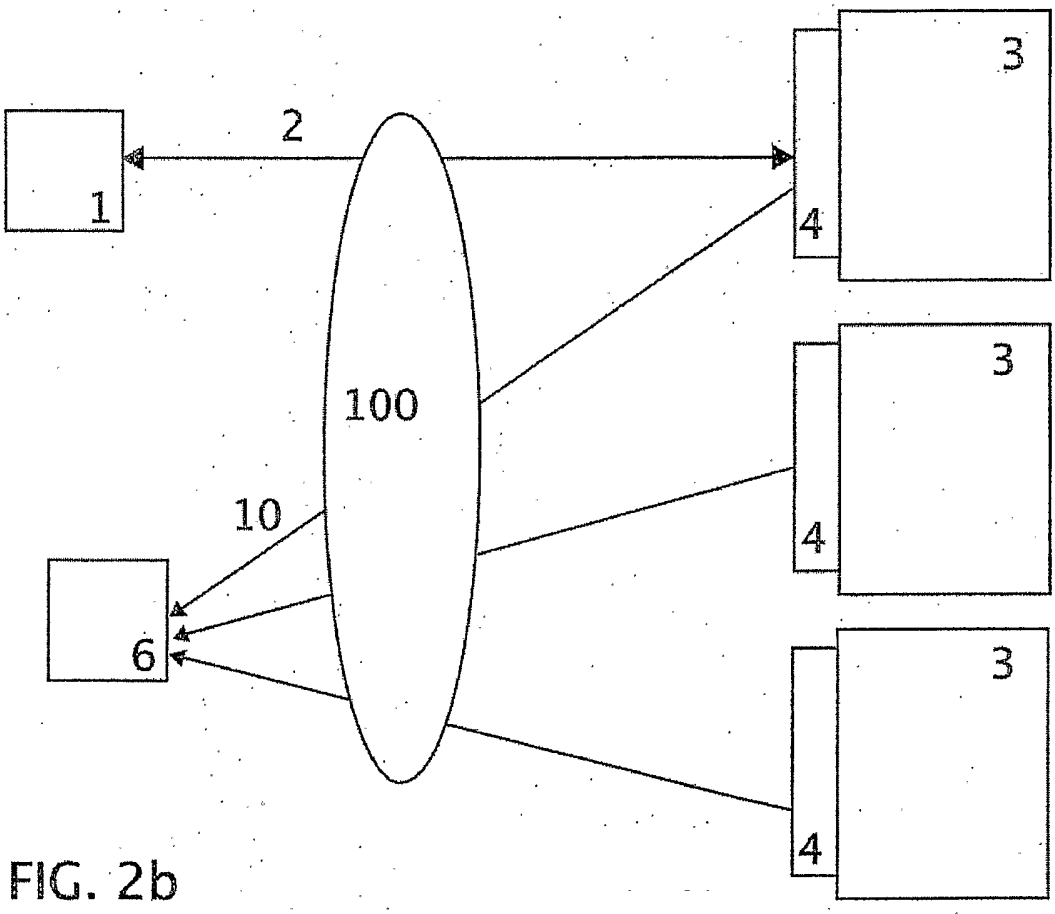


FIG. 2b

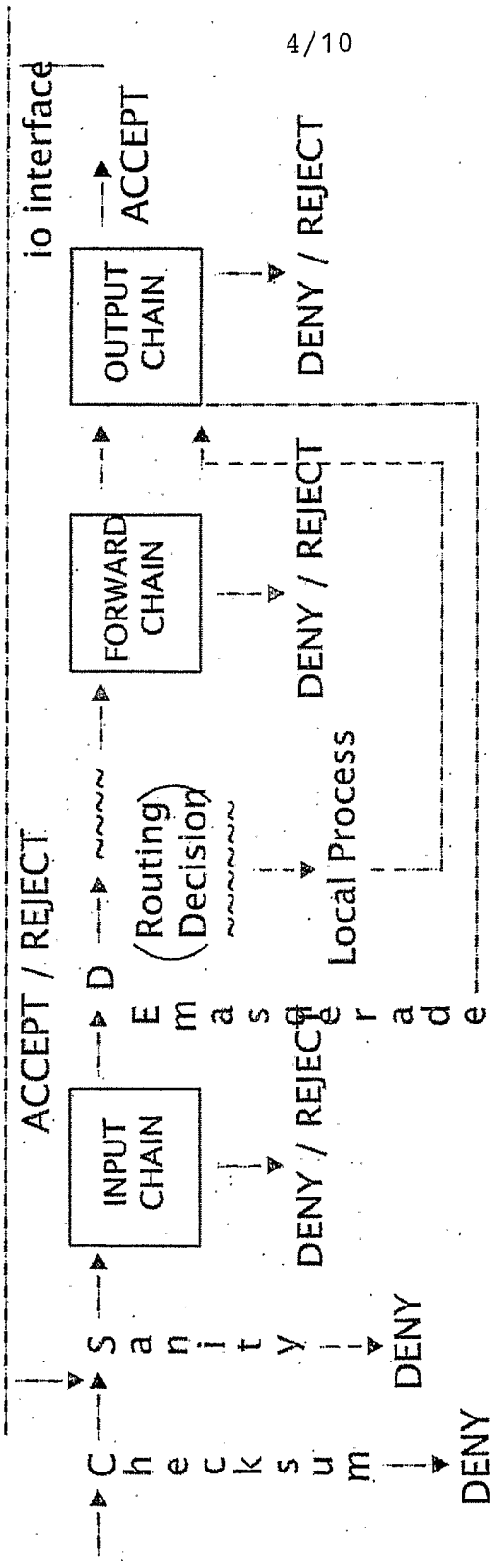

io interface
ACCEPT
OUTPUT CHAIN
DENY / REJECT
FORWARD CHAIN
DENY / REJECT
INPUT CHAIN
DENY / REJECT
ACCEPT / REJECT
Checksum
Sanity
DENY
DENY
Emaster
Decision
Routing
Local Process

FIG. 3

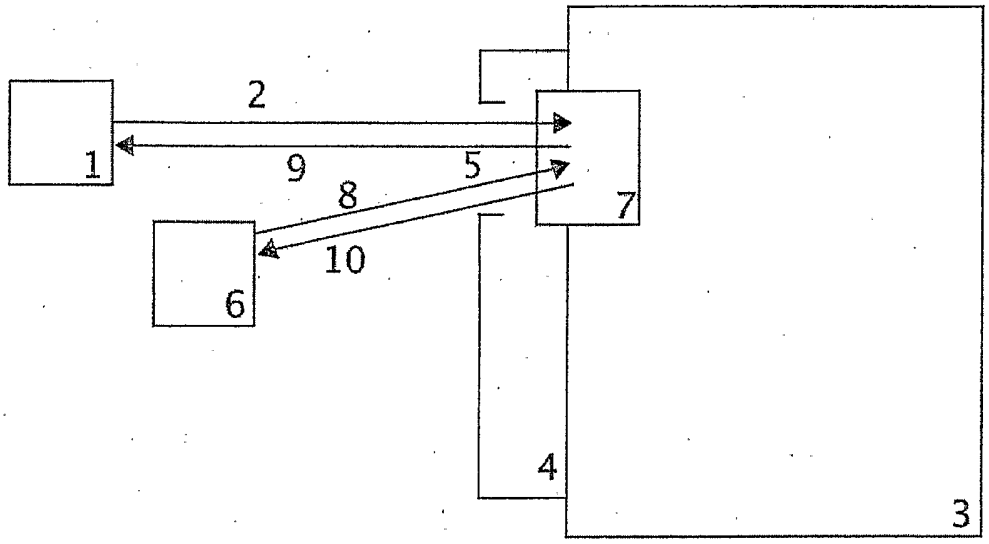


FIG. 4

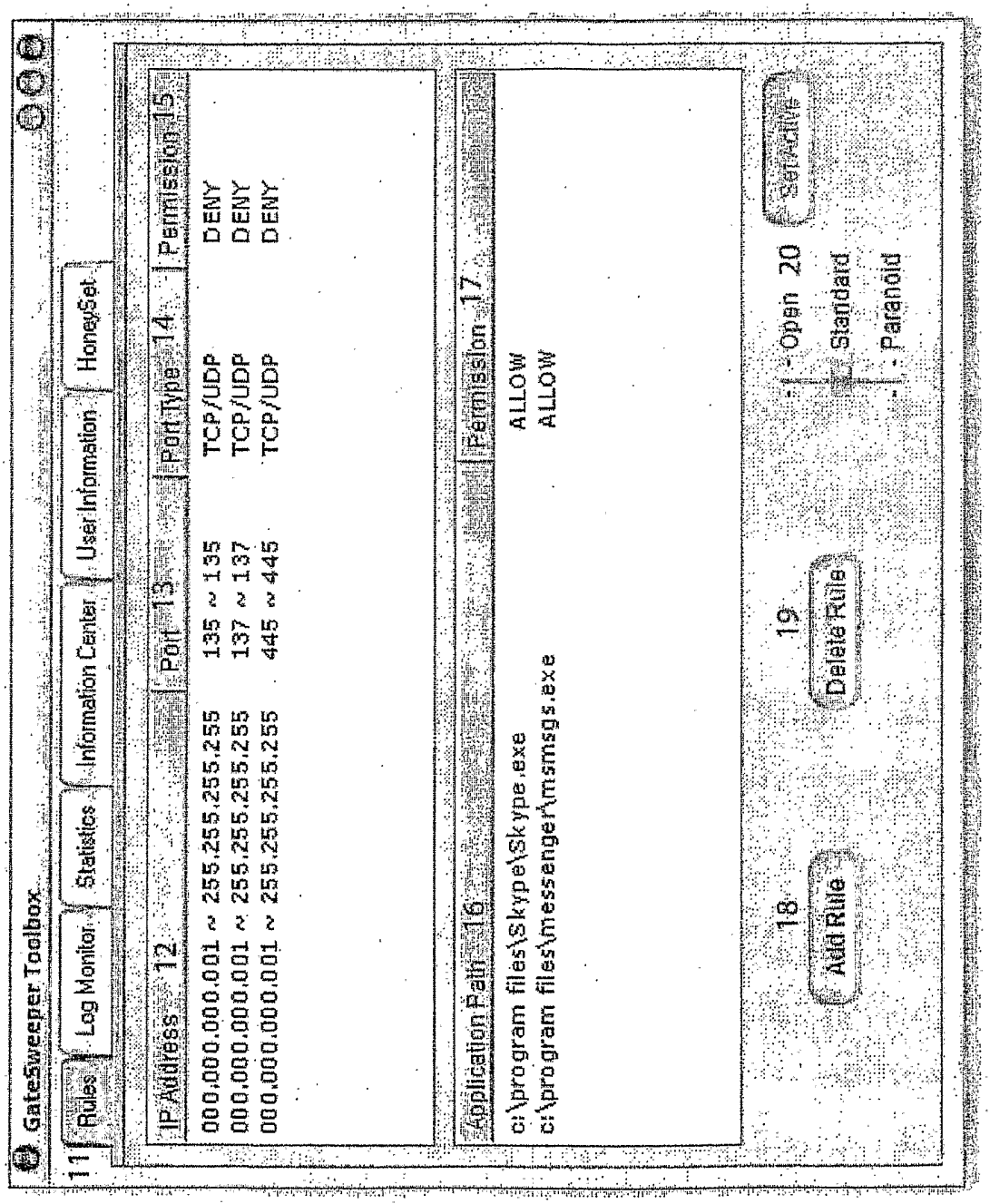

GateSweeper Toolbox
11
Rules
Log Monitor
Statistics
Information Center
User Information
HoneySet
IP Address 12
Port 13
Port Type 14
Permission 15
000.000.000.001 ~ 255.255.255.255 135 ~ 135 TCP/UDP DENY
000.000.000.001 ~ 255.255.255.255 137 ~ 137 TCP/UDP DENY
000.000.000.001 ~ 255.255.255.255 445 ~ 445 TCP/UDP DENY
Application Path 16
Permission 17
c:\program files\Skype\Skype.exe ALLOW
c:\program files\messenger\msmsgs.exe ALLOW
18
Add Rule
19
Delete Rule
Open 20
Standard
Paranoid
Settings

FIG.5

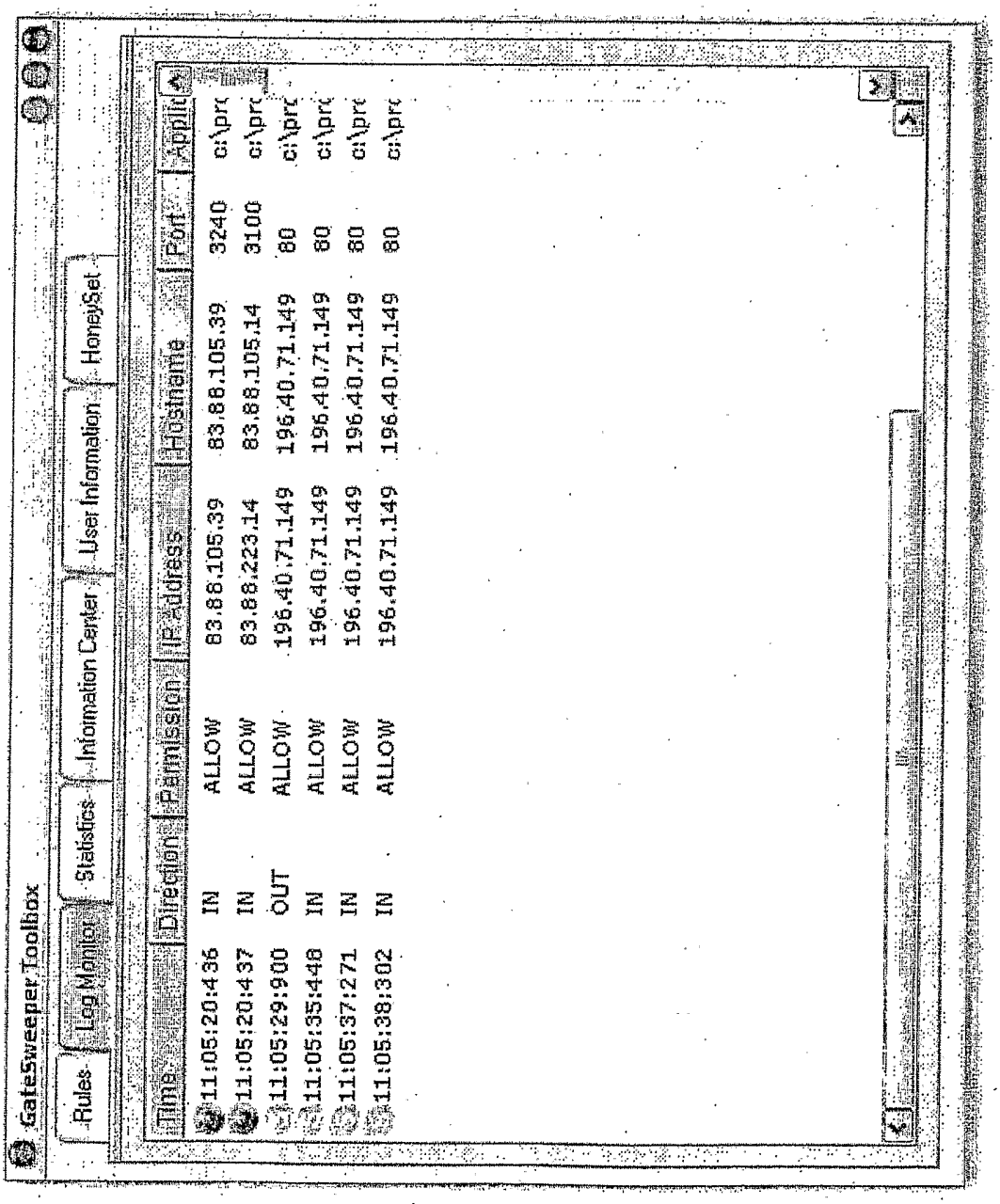

GateSweeper Toolbox
Rules
Log Monitor
Statistics
Information Center
User Information
HoneySet
Time
Direction
Permission
IP address
Hostname
Port
Applic
11:05:20:436 IN ALLOW 83.88.105.39 83.88.105.39 3240 c:\pro
11:05:20:437 IN ALLOW 83.88.223.14 83.88.105.14 3100 c:\pro
11:05:29:900 OUT ALLOW 196.40.71.149 196.40.71.149 80 c:\pro
11:05:35:448 IN ALLOW 196.40.71.149 196.40.71.149 80 c:\pro
11:05:37:271 IN ALLOW 196.40.71.149 196.40.71.149 80 c:\pro
11:05:38:302 IN ALLOW 196.40.71.149 196.40.71.149 80 c:\pro

FIG.6

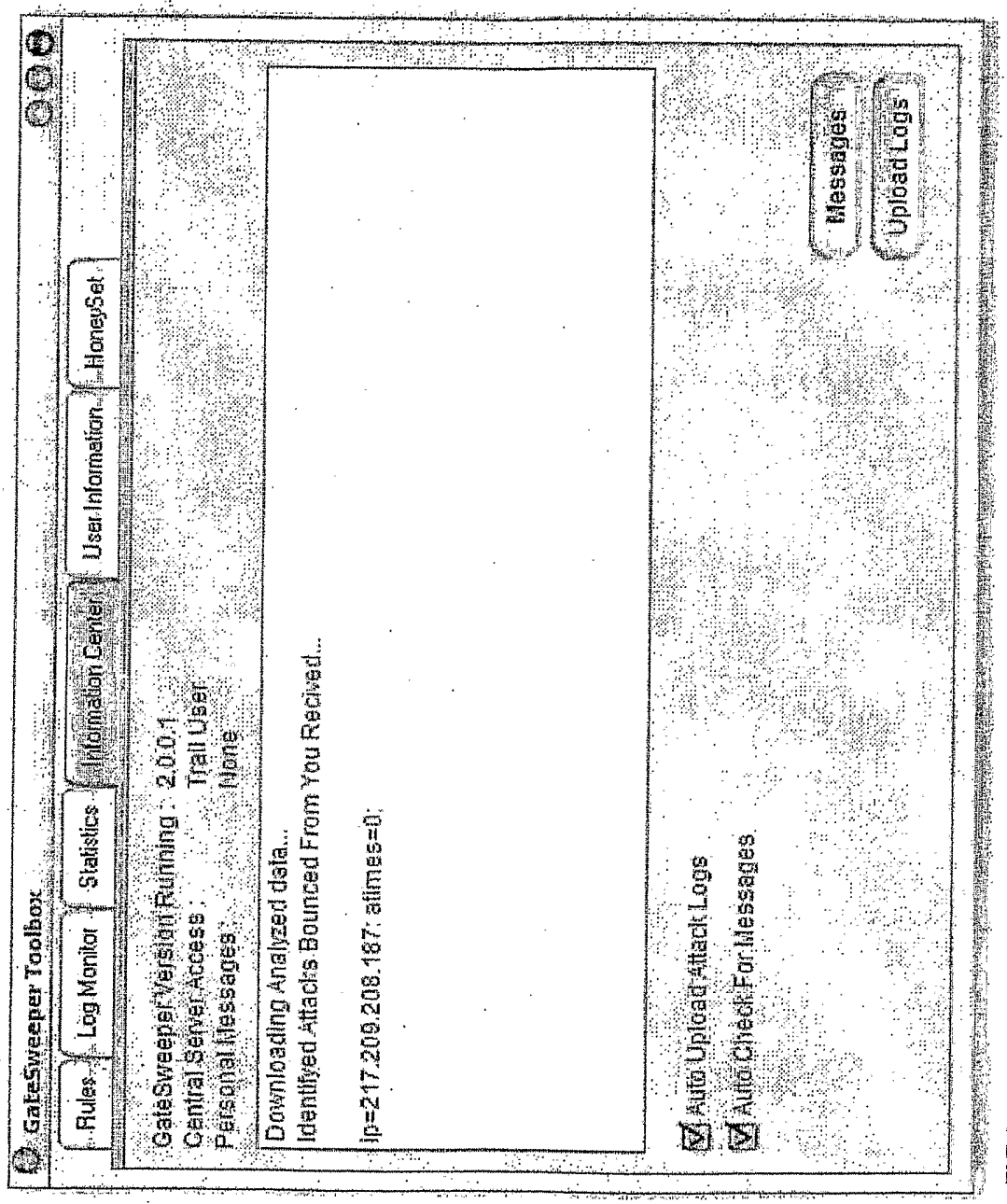

GateSweeper Toolbox
Rules
Log Monitor
Statistics
Information Center
User Information
HoneySet
GateSweeper Version Running : 2.0.0.1
Central Server Access : Trail User
Personal Messages : None
Downloading Analyzed data...
Identifyed Attacks Bounced From You Recived...
Ip=217.209.208.187: atimes=0;
Auto Upload Attack Logs
Auto Check For Messages
Messages
Upload Logs

FIG. 7

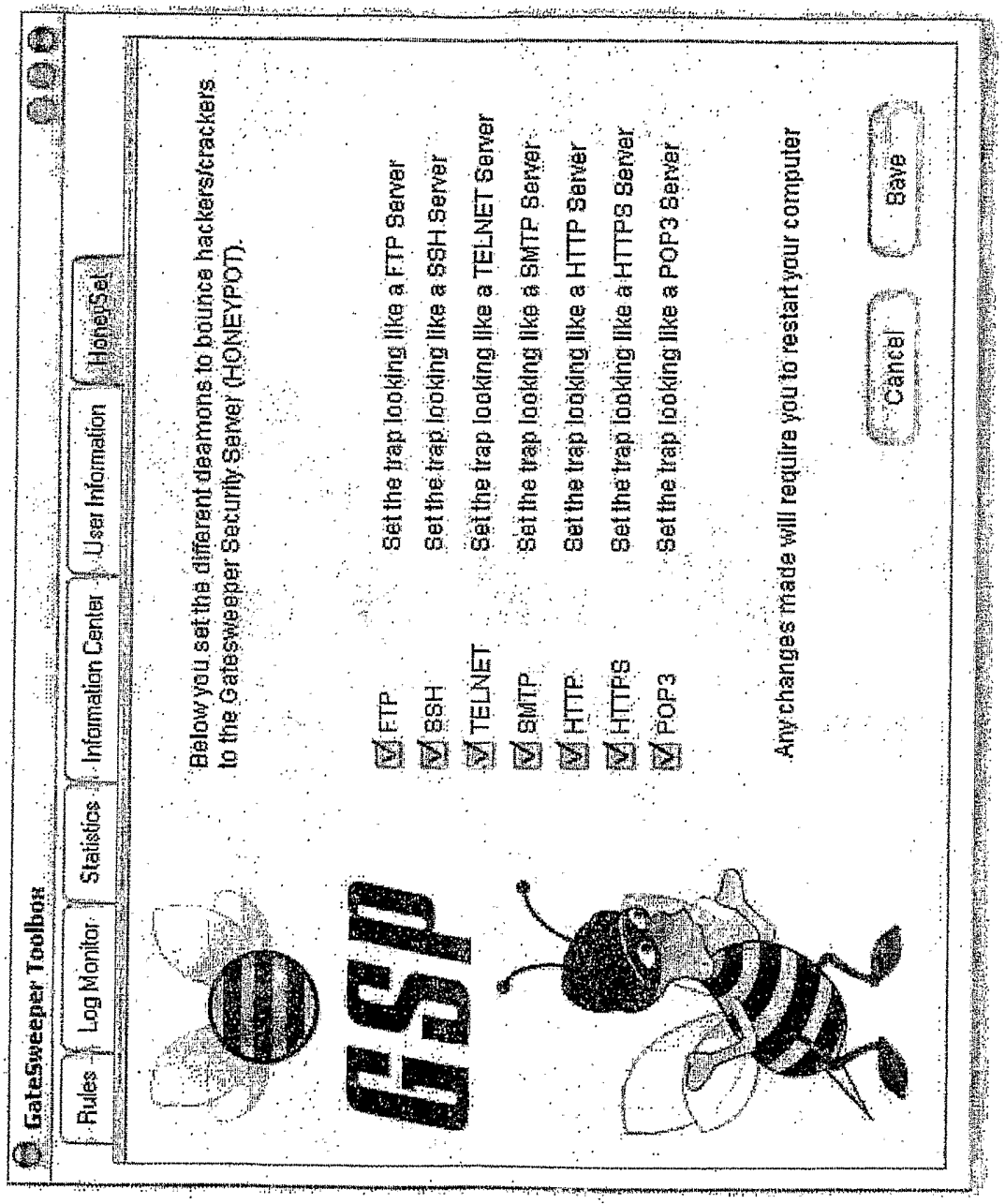

GateSweeper Toolbox
Rules
Log Monitor
Statistics
Information Center
User Information
HoneySet
Below you set the different deamons to bounce hackers/crackers to the Gatesweeper Security Server (HONEYPOT).
FTP
Set the trap looking like a FTP Server
SSH
Set the trap looking like a SSH Server
TELNET
Set the trap looking like a TELNET Server
SMTP
Set the trap looking like a SMTP Server
HTTP
Set the trap looking like a HTTP Server
HTTPS
Set the trap looking like a HTTPS Server
POP3
Set the trap looking like a POP3 Server
Any changes made will require you to restart your computer
Cancel
Save

FIG. 8

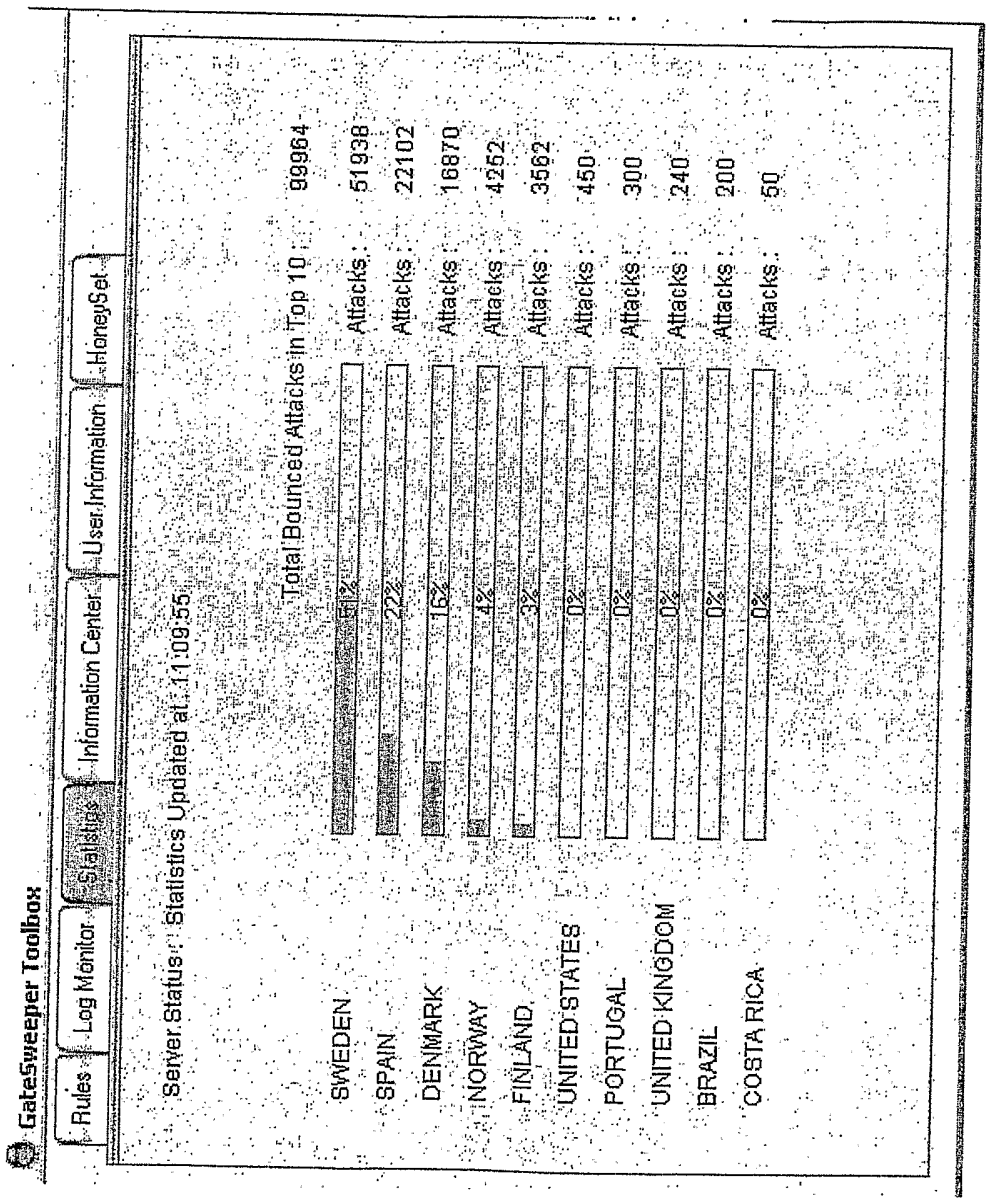

GateSweeper Toolbox
Rules
Log Monitor
Statistics
Information Center
User Information
HoneySet
Server Status: Statistics Updated at 11:09:55
Total Bounced Attacks in Top 10 : 99964
SWEDEN 51% Attacks : 51938
SPAIN 22% Attacks : 22102
DENMARK 16% Attacks : 16870
NORWAY 4% Attacks : 4252
FINLAND 3% Attacks : 3562
UNITED STATES 0% Attacks : 450
PORTUGAL 0% Attacks : 300
UNITED KINGDOM 0% Attacks : 240
BRAZIL 0% Attacks : 200
COSTA RICA 0% Attacks : 50

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/DK2006/000327

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 884 025 A (BAEHR ET AL) 16 March 1999 (1999-03-16) cited in the application column 2, line 10 - line 49 column 4, line 22 - line 27 column 5, line 56 - column 6, line 14 column 8, line 4 - line 20 -----	1-18
X	EP 1 218 822 A (GTE INTERNETWORKING INCORPORATED; GENUITY INC; GTE SERVICE CORPORATION) 3 July 2002 (2002-07-03) cited in the application paragraph [0015] paragraph [0018] paragraph [0024] paragraph [0027] - paragraph [0033] ----- -/--	1-18

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 September 2006	04/10/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Raposo Pires, João

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/DK2006/000327

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YELDI S ET AL: "Enhancing network intrusion detection system with honeypot" IEEE TENCON 2003. CONFERENCE ON CONVERGENT TECHNOLOGIES FOR THE ASIA-PACIFIC REGION. BANGALORE, INDIA, OCT. 15 - 17, 2003, IEEE REGION 10 ANNUAL CONFERENCE, NEW YORK, NY : IEEE, US, vol. VOL. 4 OF 4. CONF. 18, 15 October 2003 (2003-10-15), pages 1521-1526, XP010686929 ISBN: 0-7803-8162-9 the whole document	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/DK2006/000327

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5884025 A	16-03-1999	EP 0743777 A2	20-11-1996
		JP 9224053 A	26-08-1997
		SG 73981 A1	18-07-2000
		US 5802320 A	01-09-1998
		US 5878231 A	02-03-1999
EP 1218822 A	03-07-2002	AT 284557 T	15-12-2004
		AU 4245800 A	14-11-2000
		CA 2370135 A1	19-10-2000
		DE 60016613 D1	13-01-2005
		DE 60016613 T2	08-12-2005
		MX PA01010420 A	05-10-2005
		WO 0062167 A1	19-10-2000
		US 2005177871 A1	11-08-2005