STUDIA INFORMATICA
Nr 1/2(7) Systemy i technologie informacyjne 2006

Concept and Implementation of Module of Monitoring Condition of Scattered Computer Resources Security

Andrzej Barczak[1], Łukasz Fedorczyk[1]
[1] Institute of Computer Science, University of Podlasie,
ul. Sienkiewicza 51, 08-110 Siedlce, Poland

Abstract: In this paper the architecture of system managing security of scattered computer resources is presented.The maine functions of monitoring module are cahracterized, also its model and implementation is presented.

Keywords: computer systems' security, IDS system

1 Needs of creating systems managing computer security

Big corporations' computer systems are more and more developped and sophisticated, that is why their protection requires more complicated and refined security systems. Producers specialised in this field are trying to introduce innovative solutions enabling managing security and maitenance of such systems.These efforts are mainly directed towards:

- easy serviced, graphic, intuitive security's policy's editors,
- tools suporting analising and raporting registered incidents,
- systems visualising security's policy,
- tools monitoring condition teritorialy scattered security components.

In certain institutions, the need of introducing integrated system managing scattered computer resources' security is a must at present. Mainly, it results from rather evident grounds:

- Central consoles show graphically in syntetic form cohesion informations gathered from many physically independent localizations,
- Administrator, managing the net infrastructure is not able to make an corect decisions concerning security, becouse monitored incidents come from difrent independent of each other localizatons, in which indnvidual security components are installed for example: firewalls, systems detecting burglary etc.,

- the number of inciddents regestered by security system is very high. Limited abilities of humanbeing do not allowed to analise them efficiently without specialized tools prepered before,
- central consols managinf security allowe to rule over many information gathered from far localizations and make easier takeing an decision,
- intigration of existing elements of security managing infrastructure make it possible to reduce expences of buying products joining individual componens securing and reduceing or elimiating needs of change in working infrastructure and security's policy.

Nowadeys ther are made efforts to create central conslos managing the security, able to correlate incidents registered by definied kind of securing. The example of such a solution might be situation, in which administrator of corporational net recives an allarming information about threat to security, when definite corelation of incidents detected by security scaner, system of burglary detection IDS and firewall arrises.

2 Model of integreted system of managing scatered computer resources' security

For perpuse of beter prevention from threads to computer systems, in many institutions and companys there are created cental concols integrating components, protecting net or single host from intruders. That is similar situation to the energetic system where the aktivity of all elements is monitored and raported in manaiging place**.** For existing tools' and softwares' infrastucture of organization, the maine aime is to work out the solution in the form of model of system integreting elements of security. Such a model in a general form is presented below.

Security hardware ought to be configured to acquire a nowlage about their activity. Such a hardware makes it possible to send its log to remote computer so caled syslog server whose task is to acumulate peaces of information from difrent sources. Syslog serwer recive sent data by specialy opened UDP port, afterwards it saves data in proper files.

Programs mostly acumullate their logs in system of computer in which they are installed. This data can be saved in difrent forms: in many security tools logs are saved in data bases (for instance Microsoft Access), olso very often data are acumulated as text files.

In conection with variety of data's forms presenting activity of security components , there is a need to unify forms of information. Creating aplications combineig difent enviroments, we must creat an unific and systemated data structure – adoption of data model. The best solution is to create special data base, storing in a homogenus form logs of integreted systems. Such a solution make it easier to access and enable to montor a lot of security system's elements from angle of many features.

Data collected from many sources – from syslog server and ather hosts – are processed to unify their form and save them in appropriate table of remote data base.The structure of logs coming from monitored components concern mainly following pices information:

- accurate time of incident,
- category of incident for exmple: alert, error, warning etc.,
- the name of incident,
- accurate specification of incident for instance: IP adres, ports (bothe source and destination port), protocols etc.

In this situation one of most importand tasks of integraiting aplication is unifing forms of logs generated by independent security enviroment, in order to create an unambingouous information for monitoring unit. Unification of logs' srtucture makes that proiected data base collect information about all incidents and their atributes and about monitored security enviroments, in one form. Such a data structure in disposition of managing security system's monitor improves efficencie of monitoring elements of system's infrastructure (for instance bank corporation). Administrator of such a system can get informations about changes in component wich has an IP adres and control logs connected with defined incidents' category.

Integreted system of managing security of scattered computer's resources has got an modular architecture and embody:

- monitoring module,
- analising module,
- module managing the configuration.

Monitoring module is element making it posible to supervise activity of bank's security infrastructure. This module is acantable for conecting hardware and software. It perform following functions:

- chaking activity of montored elements, by analising changes in data sources in which logs of security software are saved,
- unifaying forms of logs to make it possible to save informations about changes in central data base,
- downloading informations about incidents from central data base based on filtr made by system's user, in aide of which administrtor can monitor defined area of system's infrastructure – concrete hardware or grup of hardwares and security software with category of incidents taking place in this components,
- extracting defined data consistent with expectations of user by defineing filters by adecuate question in SQL
- graphic and text (charts) presentation of data connected with incidents on maine managing console of security system,
- creating reports and statistics concerning activity of monitored infrastrtucture elements.

Monitoring module in a real time presents to the administrator activity of security componenys as windows set on maine panele. After activaiting system,

number determineing the frequence of questions towards the clients about actualisation of logs should be entered, what actually meens the speed of refreshing informations showed in windows.

User to be able to monitor components, must enter IP adres of machimne and choose monitored aplication: firewall, IDS or antyvirus monitor. Afterwardes server sends demand for information connected with definite components and shows them as a window. Administretor can specify what kind of incidents does he want to monitor, for example: definite categories of incidents, attacks or services. For purpose of facilitation and expansion capabilities of monitoring, user can look through statistics both in graphic and text form (thre is possibility of choosing the kind of grath: circuit or lineral).

3 Model and implementation of monitoring model

The conception and implementation of computer aplication enabling monitoring scatered security resources in one consol managing the security is presented below.

For purpuse of presenting the unifying abilities of projected software, there was choosen folowing aplications:

- ***Agnitum Outpost Firewall v. 3.5*** – aplication collecting in Microsoft Access data bases logs connected with: net connections (both bloced and not), DNS, e-mail appendixes, filtered comersials, active content of WWW pages. All of this data had been integreted and the user only has to properly configure the integratin aplication;
- ***Antyvirus system MKS_vir 2005 –*** aplication collecting logs concerning monitored activitys in text files, containeing informations about date and kind of incident which took place on the computer. All data saved in this file are used by projected aplication;
- ***Burglary detecting system Snort IDS –*** like MKS_ vir Snort saves incidents as text file. Saved are onlly this incidents which were recognised in alerts sygnature. as base of alert. They are used by projected monitoring module.

Presented components embrace only software elements of security, which can be used without big financial expenditure. It seems that hardware security systems can also be in range of such aplications.

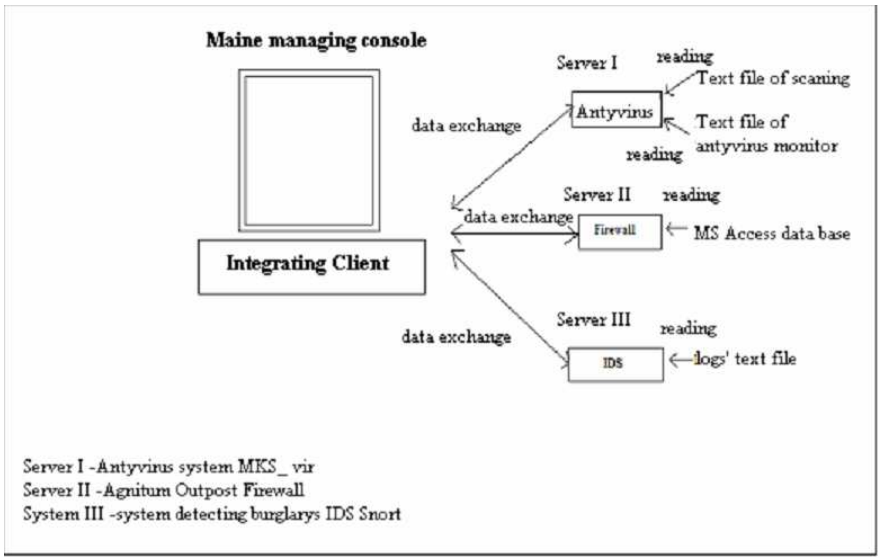
Effective monitoring of resources requires adequote configuration from angle of saveing data in local computer systems – as text files or data bases. Since then, collected data will be the base of monitoring. However, projected system is universall and he is able to integreate enother enviroments then shown above. It mainly depends on form of data saved as logs in security software: if it is comprehensible for integrating console. Informations about structure of this data are showen in requirements and project restrictions.

In purpuse of sending the containe of monitored programs' logs' diary, net system ought to be created. Projecting aplication is based on client–server architecture with use of TCP port.

Server is a program resideing on local computer, on which security resources had been instaled. That meens that server can be instaled on many machines if they posses resources requiring monitoring. The bases of server's work are configuering files, determineing basic paramets of conect, listenig for and fisical localisation of monitored logs, both in text and data base form.

From time to time console/sever aplication send requirements to the client, checking if logs' contents has changed since it was last checked. If yes, server sends to a maine monitoring console piece of information actualised by security software. As a residental program, server's aplication work in a bacground and have no influence on quality of computer's services.

The client's page is responsible for receipt data and presenting them on security menaging console. Administrator is able to supervice piece of information from 3 diferent sources. Requirement of conecting server and client is net attanablety of the components. Picture 1 showes architecture of modeled monitoring aplication.



Picture 1. Architecture of monitoring application securing computer resources

Model of data of projected module is based on stracture of data from security aplications. Server's program after properate configuration, gaines access to logs, which could be saved as text or data base. Server monitors changes in logs of supervised components and sends update entrys to a integrating client. In case of

data coming from text file, all new entrys is downloaded and send, monitored changes in data base concern only records wich are resaltes of SQL questions, asked by administrator. Data above are not procesed by monitoring aplication, that is why, defining questions turning back pieces of information desirable by user is needed.

Projected aplication is dedicated mainly for administrative aims, in range of managing security of computer resources like monitoring of net activity's condition, using security components. That means tha access to aplication and controlling it should be managed by a person responsible for administreiting the computer net of the firm.

System is diveided into two applications: client's and server's. Integreiting client has got several functions:

- autenticate by all attempts of access to maine consol,
- choice of server, whose security components are will be monitored by entering his IP and TCP adres which are controled by monitor,
- choice of source of components, whose monitoring will be presented to the user (defined SQL question from data base or defined text file),
- presenting in a real time, in the window, data collected from security resources,
- ability to download hole record from logs, for defineing aplication of security system,
- genering chart presenting ststistics of incidents noted on all components and abillity of visual edition in conformity with preferances of user.

Server progams has got following functions:

- setting the source of data – text file or data base,
- in case of data base – entering SQL comend, extracting from table defined data and their descriptions,
- ability of changing configuration by edition of configuering file or directly from aplication, however it is possible to set following parameters:
  - user's name and access pasword to a server,
  - TCP port's number, which will be listened for by server,
  - the name of security system monitor,
  - path to the catalog, in which it is instaled,
  - program's description,
  - monitored files and their descriptions,
  - data base drivers,
  - data base,
  - users' name and access paswordes to monitored data bases,
  - SQL questions and their descriptions.

How I admited before, srever's sotware is mainely based on access to data bases, in which logs of monitored programs are saved.That is why, user opening aplication first time schould configure properly server from angles of data bases. Dialog window makes it possible to enter monitored components of computer

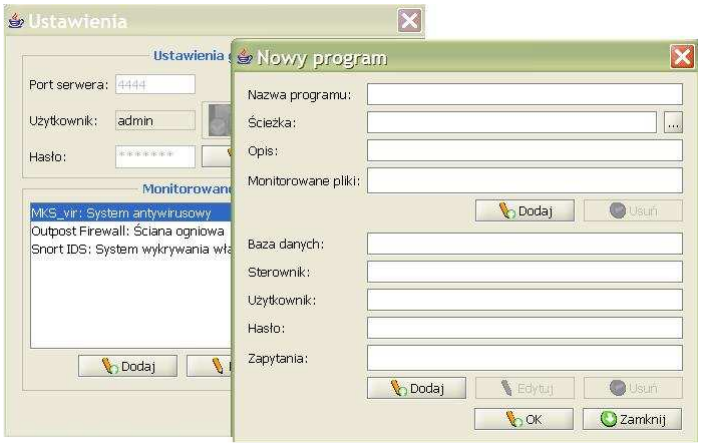
infrastructure, ending monitoringand changing access paswoard within defined unit presents picture 2.

Picture 2. Menu of configuration access to monitorem units

After pressing ***Change*** key, user is able to change server's adccess paswoard in defined computer. For this purpuse actuall paswoard schould be entered (***Old Password***), than new one (***New Password***) which ought to be confirmed (***Repeat Password***). If all this entrys are corect, aplication will change the access password. (picture 3)

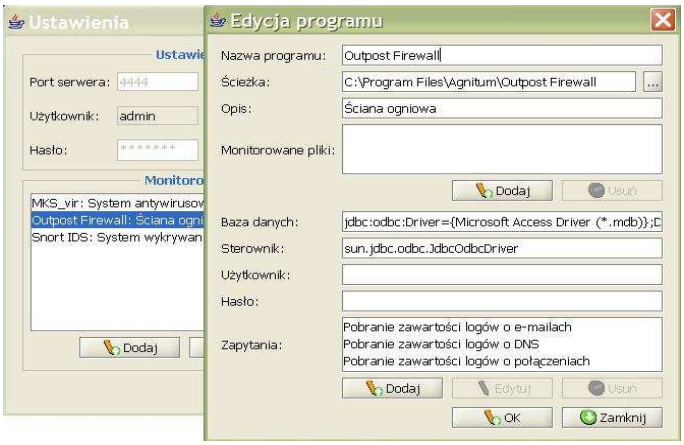
Picture 3. Changing password menu

Aplication enable the server entering monitored components by pressing ***Add*** key.(picture 2). After opening the adding new program window, user enter the name of the program (***Name of the program)*** and showes proper paths to the sources (text file or data base). Picture 4 presents window of adding new monitored unit.



Picture 4. Configuration of monitored files window- window ***New program***

Picture 5 shows editing logs of monitored program, by using ***Edit*** key.When logs of securing program are in form of text files, user shows proper path of definite file by ***Add*** in field ***Monitored files***.



Picture 5. Configuration of monitored files menu – ***Edition of program*** window

During choosing data base, user has to enter SQL questions, which will extract from chart proper data, usueful for monitoring activity of definite component. When the access to data base is protected by a password, proper values should be entered (***User*** and ***Password***).

Picture 6 presents the menu configurating SQL questions.User to insert definite question, has to know structure of the data base, in which data about condition of definite component are collected. The description of, question counting

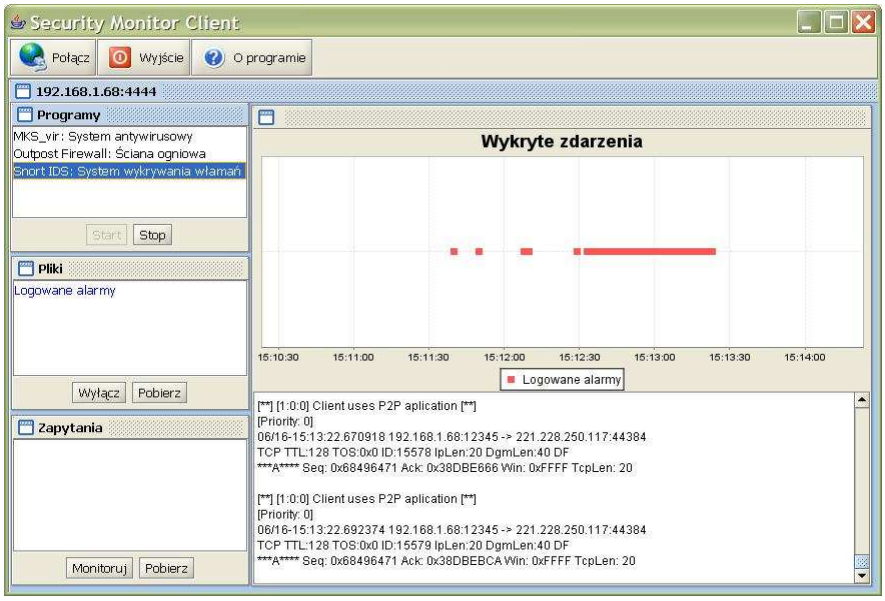
records and result question ought to be insert. Outcome of questions will be presented in client aplication, which shows monitored activity of securing program.

Picture 6. Editing SQL questions menu

Client's software is a Basic console of managing scattered computer resources. Access to a definite store is possible by entering IP adress or proper port's number, on which server application is working. It is also necessary to insert parameters of loging – user name and proper password. Picture 7 presents menu of access to a main console.

Picture 7. Loging to the server menu

After entering proper user's parameters we gain an access to a main monitoring console specialized in defined server of securing components (picture 8).

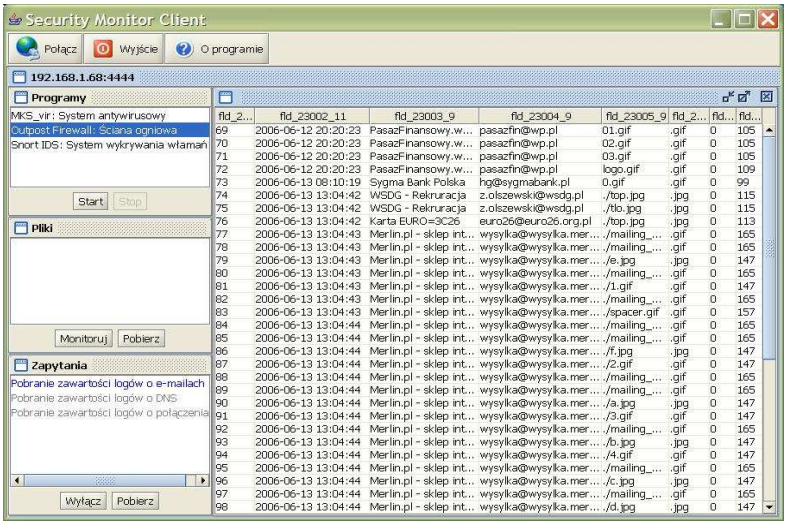


Picture 8. Menu of maine console of managment

In a left upper corner ther are componenets monitored by server. User can switch over to gain access to monitored logs. Window below consists of monitored text files, bottom window presents questions, according to which data will be send to the console.The main window showes table presenting number of incidents in time unit and content of monitored components' logs. Data presented below table are modified when the value of logs changes, that is why their actualisation is in a real time, and the user is under impresion that he manages to monitor definite element, for instance firewall.

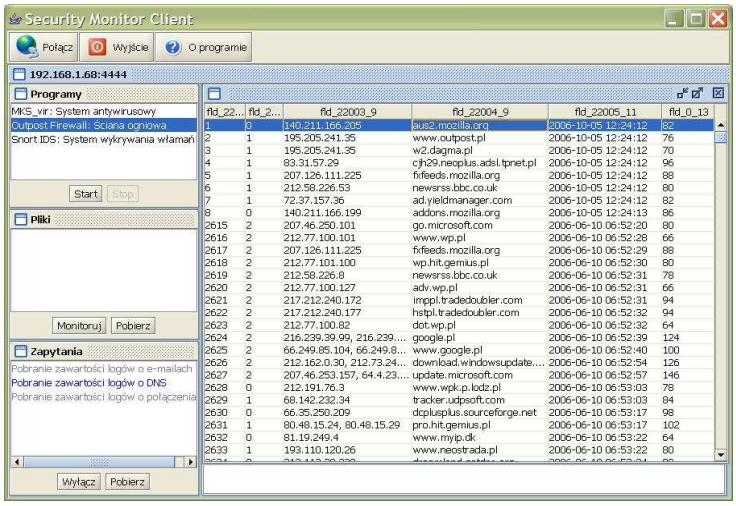
Administrator by pressing ***Download*** key can receive whole content of log files or outcome of SQL questions. Picture 9 shows downloading logs of ***Outpost Firewall*** connected with SQL questions turning back data about activity of e-mail.

Console presents outcome of SQL question definte on the server. Table containing data concerned with activity of e-mail shows accurate time of incident, subject of e-mail, e-mail address of sender, names of apendix and their extensions.



Picture 9. Examples of logs containing data about activity of e-mail

Picture 10 presents the result of SQL question concerning activity of DNS.This data concerns acurate time of incident, name of a server and its IP address.



Picture 10. Examples of logs concering information abort activity of DNS

Bibliography

1. Barczak Andrzej, Sydoruk Tadeusz: Bezpieczeństwo systemów informatycznych. Publisching of Academi of Podlasie, Siedlce 2002.
2. Broadhead Steve, Ryłko Krystian: CISCO ISR 2811-Router ze zintegrowanymi usługami. Networld, Jenuary 2006.
3. Dworakowski Wojciech: Najnowsze trendy w dziedzinie zabezpieczeń sieci informatycznych.Firewalle aplikacje, IPS, IDS In-line, matherials of IX PLOUG Conference, Kościelisko, October 2003.
4. Snort-Sieciowy System Wykrywania Włamań, http://pl.docks.pld-linux.org/usługi_snord.html
5. Test pakietów Internet Security, Computer magasine Chip 04/2005