

MODELLING RISK MANAGEMENT FOR UNIFIED THREAT MANAGEMENT SYSTEMS

Vladislavs Minkevics

Ministry of Finance, Smilšu 1,
Riga LV 1919, Latvia, Mg.sc.ing,
Vladislavs.Minkevics@fm.gov.lv

Jans Slihte

Ministry of Finance, Smilšu 1,
Riga LV 1919, Latvia, Dr.sc.ing,
Jans.Slihte@fm.gov.lv

Girts Vulfs

Riga Technical University Kaļķu
1, Riga, Latvia, Prof,Dr.sc.ing,
vulfs@itl.rtu.lv

KEYWORDS

Risk, risk management, automatic risk management, effective risk management, Unified Threat management neuron networks.

1. ABSTRACT

Minkevics Vladislavs, Šlihte Jans, Ģirts Vulfs Riska menedžmenta modelēšana unificētajām draudu apstrādes sistēmām.

Rakstā pētītas unificētās draudu apstrādes sistēmas, to pielietojšanas iespēja informācijas sistēmu riska analīzes nodrošināšanai un piedāvāts risinājums riska menedžmenta efektivitātes uzlabošanai. Lai uzlabotu riska pārvaldību nepieciešamas šādas aktivitātes: pirmkārt, ekspertam, kas novērtē informācijas sistēmu risku jābūt ar lielu pieredzi; galvenā problēma ir definēt, kuri apdraudējumi ir vissvarīgākie, ir jānosaka efektīvi risku mazinājoši līdzekļi. Otrkārt, lai pietiekami operatīvi sekotu apdraudējumiem mūsdienu IT vidē, riska analīzei jābūt nepārtrauktai, bet tā kā parasti to veic eksperts šis process aizņem daudz laika, nereti riska analīze tiek veikta tikai reizi gadā. Šajos apstākļos risku mazināšanai un rezerves nodrošināšanai jau sākotnēji jāiegulda daudz lielāki līdzekļi.

Darbā piedāvāts riska mazināšanas veids, izmantojot unificētās draudu pārvaldības sistēmas, kas balstīts uz automātisku riska analīzi, izmantojot sistēmu ģenerētos audita pierakstus. Apskatīts, kādā veidā, izmantojot standarta audita pierakstus un citas sistēmu atskaites var izveidot sistēmu, kas automātiski noteiktu riska pakāpi dažādiem apdraudējumiem un pamatojoties uz apdraudējuma nopietnības pakāpi, pieņemtu attiecīgu lēmumu par korigējošām darbībām. Riska apgabala noteikšanai var izmantot dažādas metodes, viena no tām ir neironu tīklu modeļi, ar kuru palīdzību apdraudējumi tiek klasificēti apgabalos un noteikts kāds apdraudējums kādam riskam pieder. Ņemot vērā visas iespējamās varbūtības un apdraudējumus, sistēma būs spējīga pieņemt lēmumus savlaicīgāk un efektīvāk pasargājot informācijas sistēmas no apdraudējumiem.

Minkevics Vladislavs, Slihte Jans, Ģirts Vulfs. Modelling risk management for Unified Threat Management systems

This paper addresses Unified Threat Management systems and ability to use it to analyze information risks. A solution for effective risk management is proposed. To improve risk management two basic

activities are required: first of all expert who is evaluating information risk should be very competent and experienced. Secondly, to follow threats in today's IT environment, risk analysis should be continuous, but as the matter of fact that usually it is done manually by an expert, this process is time consuming and usually risk analysis is performed once a year. In such circumstances, to minimize risk and to provide information protection and backup more funds are required.

A risk minimization method using unified threat management system which provides automatic risk management based on systems generated audit logs is provided. A review is shown on which, using system's audit log files and other system's reports, it is possible to build a system which is able to automatically evaluate risk for different vulnerabilities and according to risk level, make a decision to minimize risk. There are many methods to define risk area, one of them is neuron net's models, by using which, vulnerabilities are classified into areas and system determines which vulnerability belongs to which risk.

If all possible probabilities and vulnerabilities are put in count, system will be able to make right decisions very quickly, which will more effectively save information systems from threats.

2. INTRODUCTION

There are many ways to protect information assets. One of the most important activities is to perform comprehensive risk analysis and to define effective risk mitigation methods. Effective risk mitigation requires expert who is performing risk analysis to be very competent. Sometimes there is not enough information for an expert to evaluate one or another risk. Therefore it may be a good method to perform double risk analysis – one by the expert and another by the risk management system. Risk management system can use system's audit logs and based on pre defined risk descriptions, make a decision if it is an information risk or no.

3. PROBLEM

To create an automatic risk management system which would be able to analyze systems alarms and log files and evaluate risks, there are three main activities required:

1. system should have as much defined risk descriptions as possible;
2. system should have a defined action if there is no such defined risk in systems database, for example it may be able to teach itself;
3. decision should be made according to faults and log files.

Automatic risk management system should answer the main risk management questions and immediately inform responsible authorities if any risk exceeds the predefined value.

4. THEORETICAL ASPECTS

4.1. Risk and Automatic risk management systems

Risk is a function of the consequences (or impact) of an undesirable event and the likelihood of that event occurring. Risk assessment is the process whereby risk relationships are analyzed, and an estimate of the risk of asset compromise is developed. Compromise includes unauthorized disclosure, destruction, removal, modification, or interruption. Options for managing risk include reduction, transfer, avoidance, and acceptance. A risk assessment produces an estimate of the risk to an IT system at a given point in time. It answers the following questions:

- What can go wrong?
- How bad could it be?
- How likely is it to occur? [1]

Risk management is the process of identifying exposure risks, defining controls and requirements to manage risks, and implementing controls in a cost-effective manner. Ideally risk management should answer those questions:

- What is the risk level of each application?
- How can critical vulnerabilities be found and mitigated?
- How do infrastructure changes impact security levels?
- What is the right priority of remediation actions?

Automatic risk management system is network based system which is capable to analyze traffic, audit logs, alarms from the systems in network and by using mathematical models, make online risk assessment.

ADE risk management system:

ADE is one of the risk management systems that provide a bespoke and individual solution, which has initially been used for clients in the pharmaceutical market where good decision-making is vital but often has to be conducted against a background of incomplete information, assumptions and uncertainties. ADE combines the company's mathematical experience, skills and techniques with clients' culture and

infrastructure for efficient implementation of tailored solutions.

ADE can be designed and tailored for any situation, in any market place where portfolio management of several projects is required and where risk is associated with the projects. Solutions have been successfully implemented in a number of different companies and the organization is currently in discussions with more potential clients.

Using innovative statistical and rigorous mathematical techniques, ADE provides an environment in which to collect, process and present data through creative outputs. All this greatly helps improve client efficiency in development strategies, risk analysis and portfolio management.

ADE allows the client to make critical decisions with complete visibility of the impact of risks and uncertainties as a result of:

- Clearly mapping out different options in a structured way
- Identifying strategies which maximise financial return
- Assessing and balancing risk and return
- Focussing on high level issues
- Having confidence in the mathematical analysis [2]

Risk view system:

RISK-VIEW is another known risk management tool for the process industry, developed and patented by 7-Technologies. Knowledge of past, present and expected events forms the basis for RISK-VIEW predictions of how your process will perform in the future. At the same time RISK-VIEW will give you advice on how to solve potential problems arising tomorrow, in a week or even a month from today. RISK-VIEW can predict and inform, on the basis of information from the pumping stations, when the extra load will reach the plant. RISK-VIEW will warn the operator in advance of how to prepare for the situation. RISK-VIEW's capability of predicting future problems is obtained by combining a traditional fault tree analysis with data that are already fully available in your company.

The traditional fault tree analysis is a static method for calculating the consequence of certain events. The analysis provides an overview of complex systems and defines the combinations of faults leading to an unwanted consequence.[3]

4.2. Unified Threat Management systems

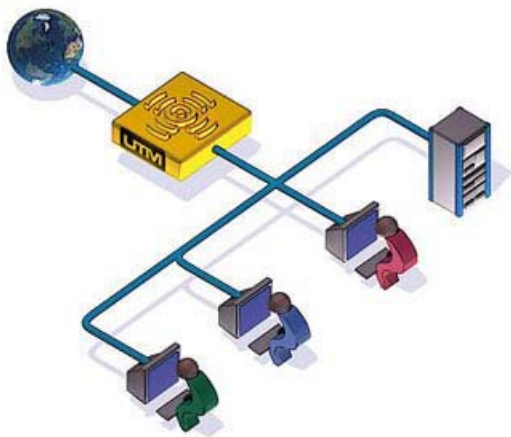
Unified Threat Management is the name for an emerging trend in the firewall appliance security market. You might say that Unified Threat Management is a system that performs content filtering, spam filtering, intrusion detection and anti virus duties that traditionally are handled by multiple systems.

When hackers were the primary focus of the IT Enterprise, a good solid firewall was sufficient to

protect a network. Then as viruses became more prevalent we installed Anti Virus Gateways that scanned for viruses and soon web content filtering and then spam filtering. This resulted in a mess of systems that were costly to administer and consumed valuable rack space.

As the hardware that powered today's enterprise firewalls became more robust it became viable to add these off box functions right into the firewall. Firewalls became "Firewall Appliances". This is where Unified Threat Management comes in. Rather than administer multiple systems that handle Anti Virus, Content Filtering, Intrusion Detection and Spam Filtering, companies can purchase a Unified Threat Management Firewall Appliance that integrates all of the above into a single rack mountable network appliance. The greater functionality that the Unified Threat Management Firewall Appliance provides can be the justification for the replacement of older more basic Firewalls in favor of a Unified Threat Management firewall appliance that does it all. [4]

For instance UTM intrusion prevention system uses over 2500 rules and signatures to identify attacks. The system actively intervenes in the data stream and blocks attacks before they can infiltrate the network. A special Auto-Prevention function simplifies configuration and thereby enables rules and rule groups to be quickly adapted to different security needs in the protected systems. UTM Vulnerability Scanner specifically checks protected systems for vulnerabilities. PacketAlarm continuously runs tests and lists the vulnerabilities it finds. In addition to being well structured, these lists present detailed information on any vulnerabilities found and recommend how they can be removed. [5]



Picture 1 „UTM’s location in network”

The emerging Unified Threat Management Security Appliance market transforms single function appliances into a more flexible environment for deploying multiple security features on a single platform. Unified Threat Management systems are quickly gaining popularity

because they offer security application performance, operating cost savings, and capital cost preservation.[6] It is understood that nowadays systems become more integrated and available to communicate between each other. Unified Threat Management systems can provide a valuable information for automatic risk management system, because viruses and intrusions are the main threats that are affecting information systems.

5. WHY INFORMATION TECHNOLOGY AUTOMATIC RISK MANAGEMENT SYSTEM

Organizations that are taking care of their information systems, usually are taking risk assessment. Manual risk assessment has some disadvantages:

- this method of risk assessment requires experts to be very competent;
- it is hard to create one list of vulnerabilities to include needs of all systems;
- the risk assessment is based on subjective thoughts of the members of expert group;
- risk assessment is time-consuming procedure, if risk assessment has to be done for 5 information systems, it may take a few days;
- because it is time consuming, usually it is done once a year, which may cause much vulnerability to be unnoticed, before they happen.

To avoid these disadvantages, risk assessment could be divided into two parts:

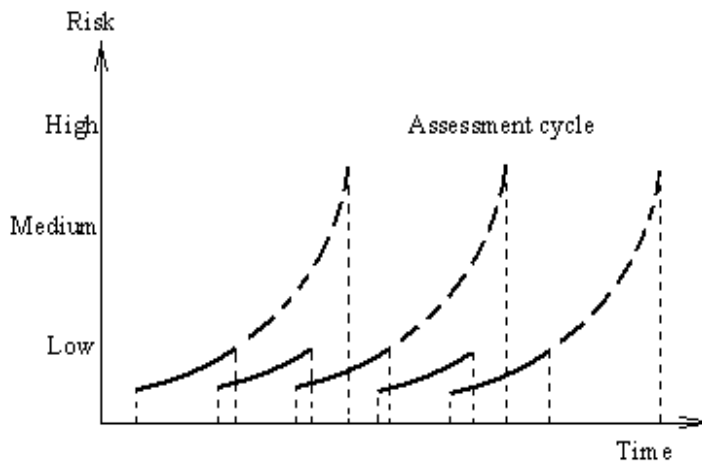
- risk assessment using experts;
- risk assessment done by the system.

Because automatic systems are not able to evaluate all possible risks, it would be very useful to leave manual risk assessment and combine it with reports from automatic risk assessment systems. For instance if Contingency and recovery plans are being evaluated. All aspects should be covered, including:

- back-up practice and policy;
- the contents of the recovery plan;
- the status of the recovery plan;
- the recovery location;
- general contingency practice, procedure and policy;
- network contingency;
- application contingency.[7]

Picture 2 shows that there is direct correlation between the risk assessment cycle time and risk level. The longer the assessment cycle time the more exposed is the organization is to attacks on critical information assets. Therefore, the most straightforward way to reduce risk is by completing the assessment cycle much faster . It will shrink the window of exposure.

By using automatic risk assessment it is possible to shrink exposure to a single day.[8]

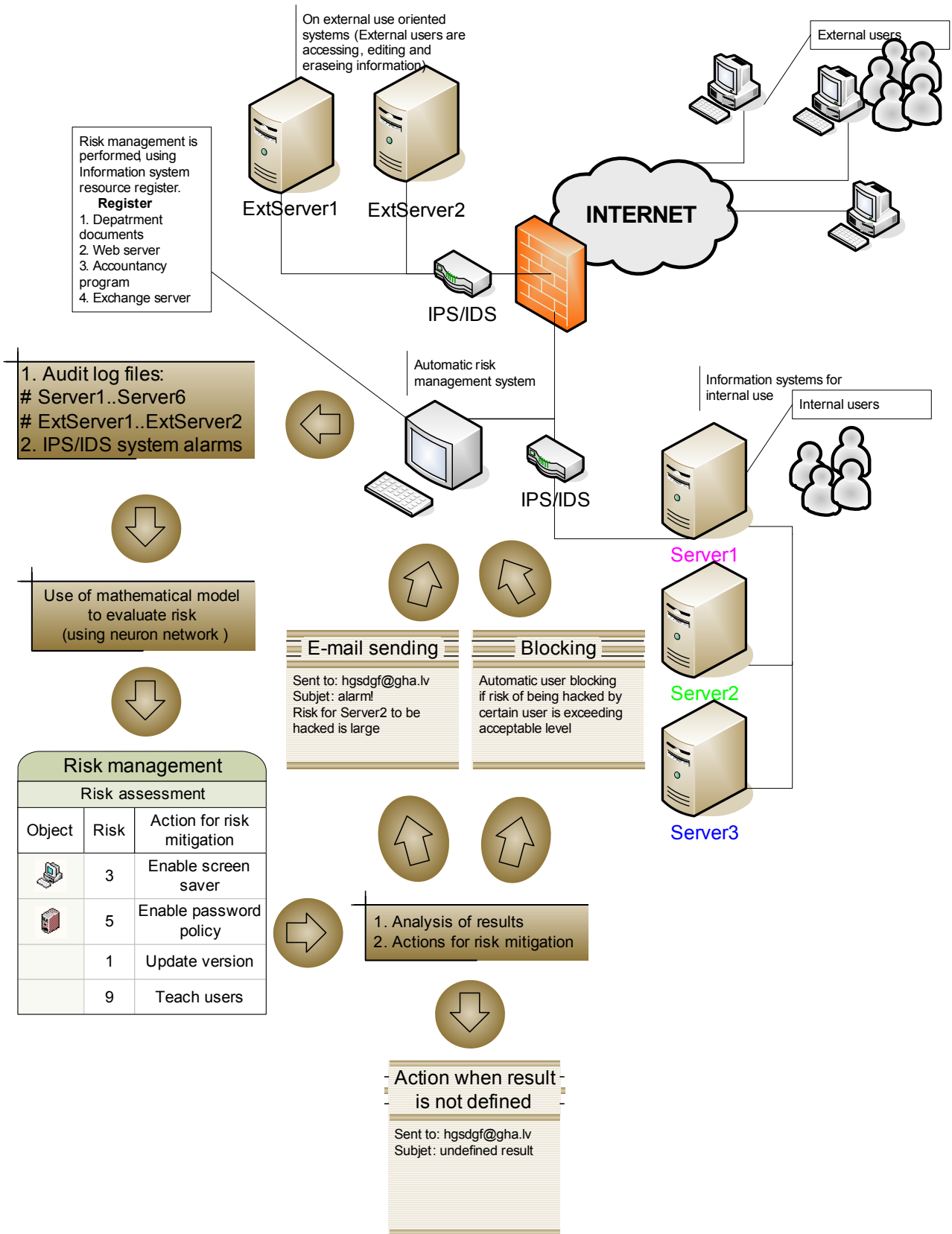


Picture 2 "Risk assessment cycle"

As it was previously mentioned, there are a few automatic risk management systems known but information system risk management system is not available for organizations yet. Information systems automatic risk management system would be a very helpful tool for information system holders and security managers to get a full picture of security risks in organization and to improve security before unwanted security event occur.

On picture 3 information systems automatic risk management system's location in the network is shown. Main parts of the system are mathematical analyzer. One of the options for mathematical analyzer may be neuron network, such as Delta learning rule and decision making algorithm. The main advantage of delta learning rule is that expert who is creating all rules for automatic risk management system may define main properties of each vulnerability and system will automatically sort them into classes from which we can gain risk level of one or another threat.

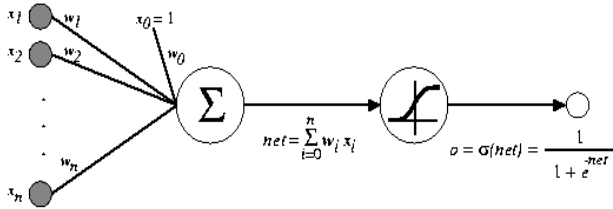
6. MODEL OF AUTOMATIC INFORMATION TECHNOLOGY RISK ASSESSMENT SYSTEM.



Picture 3 „Scheme of information systems automatic risk management tool”

7. MATHEMATICAL MODEL (NEURON NETWORKS & DELTA LEARNING RULE)

Neuron network seems to be very sufficient solution to sort threats by different criteria's. Delta learning rule seems to be suitable for this task. On picture 4 it is delta learning rule shown.



Picture 4 „Delta learning rule”

learning signal is calculated as follows:
 $r = [d_i - o_i] f'(net_i)$, where d_i is purposed neuron reaction.
 o_i is real neuron reaction.

$$o_i = f(net_i) = \frac{2}{1 + e^{-\lambda net}} - 1$$

$f'(net_i)$ – result of activation function, which is calculated for $net = w_i^t x$

Algorithm will stop when error

$$E = \sum_{i=1}^I E_i = \sum_{i=1}^I \frac{1}{2} (d_i - o_i)^2$$

had reached an acceptable level.

To minimize the error level, changes in weights will be made this way:

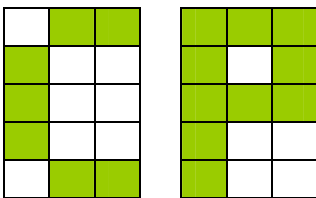
$$\Delta w_i = c(d_i - o_i) f'(net_i) x$$

Where c is randomly selected constant value.[9][10]

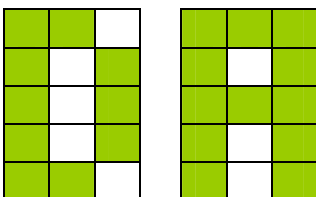
For instance:

There are 2 classes with 2 symbols in each class

1. class



2.class



Symbol classification is shown in Table 2. Using this classification rules will be created.

Table 2 “Symbol classification”

	Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9	Y10	Y11	Y12	Y13	Y14	Y15	Y16
C	0	1	1	1	0	0	1	0	0	1	0	0	0	1	1	1
P	1	1	1	1	0	1	1	1	1	1	0	0	1	0	0	1
D	1	1	0	1	0	1	1	0	1	1	0	1	1	1	1	0
A	1	1	1	1	0	1	1	1	1	1	0	1	1	0	1	1

Teacher's answers are:

C	1	1	-1
P	1	-1	1
D	1	-1	1
A	-1	1	1

Beginning weight values are:

$W_1 = (0,2;0,2;0,2;0,2; 0,2;0,2;0,2;0,2; 0,2;0,2;0,2;0,2; 0,2;0,2;0,2;0,2)$

$W_2 = (0,1;0,1;0,1;0,1; 0,1;0,1;0,1;0,1; 0,1;0,1;0,1;0,1; 0,1;0,1;0,1;0,1)$

$C = 1;$

$\lambda = 1;$

$E_{min} = 0,01$

C symbol

$Net_{11} = 1,6$

$o_{11} = (2/(1+\exp(1,6)))-1 = 0,664$

$\Delta w_{11} = \lambda(d_{11} - o_{11}) * 0,5 * (1 - o_{11}^2) = 0,28$

$E = 0,5 * (d_{11} - o_{11}) = 0,5(1 - 0,28) = 0,056$

Iterations will continue for each symbol until Error level reached acceptable level. For our example it is 0,01.

When error level will be 0,01 or less the algorithm will stop. In this case algorithm stops at 26th iteration.

As a result we gained weights:

$W_1 = -0.088; 2.639; 0.147; 0.809; 0.300; -0.088; 0.809; -3.046; -0.088; 0.809; 0.300; -2.856; -0.088; -4.155; -2.622; 0.809$

$W_2 = -1.686; -1.860; 1.462; 0.308; 0.200; -1.686; 0.308; 2.871; -1.686; 0.308; 0.200; 1.188; -1.686; -2.363; 4.336; 0.308$

This means that by putting these weights in system, it will recognize the object (which class it belongs to).

8. PRACTICAL USE USING SELF LEARNING NEURON NETWORKS

Practically this automatic online risk evaluation will be tested on the system where many different signals are analyzed. The main signal to be tested is audit log files from the server with very important information in it. The most important audit files that should be analyzed online is file server's security audit log files (Table2).

Table 2 “Example of audit log file”

Audit log ID	Description	User	Comments
560	Security: Object Access	Pa-upite	ReadData (D:\DATA_PA\vd_sa n.doc
560	Security: Object Access	En-lipsa	DELETE D:\Users\En\En-lipsa\Twin_Status.xls
540	Security: Logon/Logoff	BJ-vitol	Kerberos; 121.210.15.23
3006	Application: Warning	EvntAgnt	Error reading log event record
532	Security: Logon/Logoff	Ai-vaiva	The specified user account has expired 121.210.15.223
576	Security: Privilege Use	Kj-guran	SeChangeNotifyP rivilege

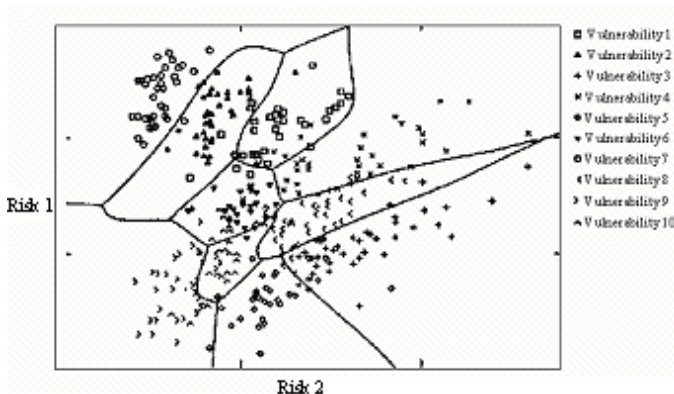
The main problem is to sort important audit logs from not so important ones. Very skilful experts are needed to prioritize logs. When it is done, using advantages of neuron network it should be put in a system in numeric format:

Table 3 “Classes of risk evaluation”

Class	#1	#2	#3	#4	#5	#6	#7	#8
1	1	0	1	0	1	1	0	1
2	0	1	1	1	0	1	0	0
3	0	1	0	0	1	0	1	1

Risk is calculated by dividing possible vulnerabilities into classes. For example in Table 3, there are two classes or two risk definitions: 1) Possibility of being hacked. 2) Password limitation is too strict. As to numbers #1 to #8: they mean different vulnerabilities, like - #1 user tried to enter password three times; #2 very limited access object has been accessed; #3 network traffic is more than 50% for more than 15 minutes; etc.

After using Delta learning rule, we have got weights to recognize an object. By putting these weights into formula $net = w_i \cdot x$ it is possible to tell which vulnerability belongs to certain risk object.



Picture 5 “Risk identification using neuron networks”

The identification of risks is shown on Picture 5, here, vulnerabilities are defined as small dots on xy axis. Each vulnerability, according to delta learning rule’s defined classification belongs to one or another risk (risk is shown as areas). The main task is to create the correct rule and to classify vulnerabilities according to defined algorithm. Even if vulnerability is not defined, system will classify it by the knowledge it gained before, which means it will be able to classify new vulnerabilities.

9. CONCLUSIONS

The proposed system will be able to teach itself and effectively make decisions which vulnerability can be addressed to which increase of risk value.

For a system where this solution is proposed, there are a few problems that might slow the implementation of automatic risk management:

- Not all systems are creating log files (some of them are old),
- Not all audit files are the same format (program or tool is needed to make log files understandable for automatic risk assessment system).

This means that at first, the most important systems should be able to create audit files.

At the moment automatic risk analysis system is in developing phase and there are many things that are not noticed yet, and will be slowing its integration in organizations risk management procedure. If everything goes well, it is possible to get a system that will start really effective risk management in organization and save money by preventing risks rather than fighting with consequences.

References

1. V.Minkevics and J.Slihte Riga 2004 “Computer science” Science proceedings of Riga Technical university; Series 5; ISSN 1407-7493;
2. St. John’s Innovation Centre Ltd http://www.ircnet.lu/matching/completerec.cfm?BBS_ID=13s843&COMPANY=102381
3. Seven technologies <http://www.7t.dk/riskview/download/rv-brochure.pdf>
4. Unified Threat Management Firewall Appliances <http://www.unifiedthreatmanagement.com/>
5. 2003 FORTINET INC <http://www.fortinet.com/news/pr/2004/pr092204.html>
6. VarySys Technologies http://www.packetalarm.com/packetalarm/index_utm.php
7. 2003 C & A Security Risk Analysis Group <http://www.security-risk-analysis.com/cobkbs.htm>
8. “Information Systems Control” Volume1 2005 “The Role of Attack Simulation in Automating Security Risk Management” by Gidi Cohen
9. Erik Postima IKAT Universiteit Maastrich www.cs.unimaas.nl/~postma/DMcourse/DM.ppt
10. <http://www.abo.fi/~rfuller/nfs10.pdf>