INFORMATION SECURITY COMPANY IN A DOS (DDOS) ATTACK

Valerie Lahno

Lugansk National Agrarian University, , Lugansk, Ukraine

Summary. The article to contain results of the researches, allowing to raise level of protection of the automated and intellectual information systems enterprises (AIS). The article discusses the use of discrete procedures to detect threats DoS (DDoS) attacks for information resources.

Key words: information security, threat detection, discrete process.

INTRODUCTION

The influence of information automation systems pervades many aspects of everyday life in most parts of the world. In the shape of factory and process control systems they enable high productivity in industrial production, transport systems they provide the backbone of technical civilization [Slobodyaneuk M. 2010]. One of the foremost transport businesses security concerns is the protection of critical information, both within their internal financial infrastructures and from external elements. Up to now, most of these systems are isolated, but for the last couple of years, due to market pressures and novel technology capabilities, a new trend has been rising to interconnect automation systems to achieve faster reaction times. Initially, such interconnections were based on obscure, specialized, and proprietary communication means and protocols. Now more and more open and standardized Internet technologies are used for that purpose. Studies show that most cyber-attacks occur inside organizations, instigated by personnel with valid access to the system. This work describes the design, implementation, and testing of a security system that enhances the capability of transport businesses to protect information within the boundary of their networks.

The sophistication and effectiveness of cyber attacks have steadily advanced. These attacks often take advantage of flaws in software code, use exploits that can circumvent signature-based tools that commonly identify and prevent known threats, and social engineering techniques designed to trick the unsuspecting user into divulging sensitive information or propagating attacks. These attacks are becoming increasingly automated with the use of botnets - compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots) have become a key automation tool to speed the infection of vulnerable systems [Ahmad D. 2005, Chi S.-D. 2001, Gorodetski V. 2002, Knight J. 2002, Templeton S. 2000, Xiang Y. 2004].

RESEARCH OBJECT

Mission-critical information systems (MCIS) are understood as the electronic communication development objects, by means of which collection, processing, storage and transmission of information are performed with the purpose to ensure the handling processes. Their exceedance of allowable values may lead to the malfunction or their endamagement. Managing critical applications and infrastructures, or operating critical solutions, requires a secure and safe but flexible service to meet the specific business needs. The CIOs of enterprise should implement management controls to verify that system owners reporting, particularly on mission-critical systems, are developing system contingency plans. Similarly, the Component CIOs should implement controls to ensure that system owners are conducting recurring tests of the systems plans.

RESULTS OF RESEARCH

The Distributed Denial of Service (DDoS) attacks against major Internet sites in 2009-2011 years highlighted the urgent need for improving the security of networks and systems connected to the Internet. According to statistics for 2011 [11], 89% of DDoS traffic was generated in 23 countries. The distribution of DDoS sources was fairly evenly spread among those countries, with each accounting for 3-5% of all DDoS traffic. Most attacks came from the US and Indonesia with each country accounting for 5% of all DDoS traffic. The US's leading position is down to the large number of computers in the country. Last year, US law enforcement authorities waged a successful anti-botnet campaign which led to the closure of a number of botnets. It is quite possible that cybercriminals will try to restore the lost botnet capacities and the number of DDoS attacks will increase. Meanwhile, the large number of infected computers in Indonesia means it also ranks highly in the DDoS traffic rating. In 2011, almost every second machine (48%) on the Indonesian segment of Kaspersky Security Network, Kaspersky Lab's globally-distributed threat monitoring network, was subjected to a local malware infection attempt. Such a high percentage of blocked local infection attempts is the result of a large number of unprotected computers being used to spread malware. Those countries responsible for less than 3% of all DDoS traffic included countries with high levels of computerization and IT security (Japan, Hong Kong, Singapore) as well as countries where the number of computers per person is significantly lower and antivirus protection is far from perfect (India, Vietnam, Oman, Egypt, the Philippines, etc.).

The decision of questions of complex maintenance of security and stability of functioning of the automated systems (AS) in the conditions of unauthorized access (UNA), including, influences of computer attacks, demands the system analysis and synthesis of possible variants of construction of means of counteraction UNA means. At complex formation it is necessary to co-ordinate and inter connect functions and parameters of the EXPERT, protection frames of the information from UNA, anti-virus means, gateway screens, the communication equipment, the general and special software and perspective means of counteraction to computer attacks.

In the aftermath of the DDoS attacks, security experts identified network intrusion detection as one of several technologies that can lead to improved network security. While intrusion detection processes alone cannot prevent or defend against security attacks, they can serve as a valuable source of information for security administrators about the types of activity attackers may be using against them. Network intrusion detection (NID) is the process of identifying network activity that can lead to the compromise of a security policy [Smirniy M., Lahno V., Petrov A., 2009].

Two primary forms of network intrusion detection systems (NIDS) exist: misuse detection and anomaly detection. Misuse detection relies on matching known patterns of hostile activity against databases of past attacks. Although they can be quite effective at identifying known attacks and their variants, misuse detection systems are generally unable to identify new security attacks and also require ongoing threat database updates in order to remain effective. Anomaly-based NID identifies malicious activity by applying statistical measures or artificial intelligence to compare current activity against historical knowledge of network utilization. Common problems with anomaly-based systems are that they often require extensive training data for artificial learning algorithms, and that expert systems quickly become overwhelmed with the number of rules required to identify all potential network threats Chowdhury M., 2004].

The Fuzzy Intrusion Recognition Engine (FIRE) is an anomaly-based intrusion detection system (IDS) that uses fuzzy systems to identify malicious network activity. The system combines simple network traffic metrics with fuzzy rules to determine the likelihood of specific or general network attacks. FIRE relies on fuzzy network traffic profiles as inputs to its rule sets. Although FIRE is not exclusively a network-based detection system, we will focus on network profiling for this paper. The FIRE goals are:

- To demonstrate how fuzzy systems can be used as an intrusion detection method.
- To identify which data sources that are the best inputs to the fuzzy intrusion detection system.
- To determine the best methods for representing network input data.

• To show how the system can be scaled to distributed intrusion detection involving multiple hosts and/or networks.

The first stage of modeling fuzzy knowledge bases consisting of the formation of expert information for the object model by constructing a knowledge base. This is the traditional fuzzy systems and does not guarantee the match and model desired result. The second stage required for tuning of fuzzy models through its learning from experimental data. Training model is the selection of parameters of membership functions by minimizing the difference between the experimental and theoretical data.

The data mining process effectively reduces the size of the data that needs to be retained for future comparisons. The NDP prepares counts and other statistical measures from the mined data and stores them to disk. Since FIRE is an anomaly detection system, the measures are chosen such that anomalies in network data can be ascertained easily. Typical summaries include [Lahno V., A. Petrov A., 2009]:

1. The number of total packets observed in the data collection interval.

2. The number of unique sdp's observed in the interval.

3. The number of sdp's that are new in this data collection interval.

4. The number of sdp's that are new in the longerterm data retention interval (i.e. have never been seen before).

5. The number of well-known ports used in an interval.

6. The variance of the count of packets seen against the sdp's.

7. The number of sdp's that include foreign hosts (hosts outside the local network domain).

8. The number of successfully established TCP connections in a time interval.

Analytical model of membership function of variable ϕ (ϕ - controlled input variables) to an arbitrary fuzzy term T can be expressed as

$$\mu^T(\phi) = \frac{1}{1 + \left(\frac{\phi - \alpha}{\beta}\right)^2}, \qquad (1)$$

where: α - coordinate of the maximum function; β - the coefficient functions.

Function of the controlled parameter ϕ_i fuzzy set of values conducive to the realization of the j-th option, describe the function (S-Q)-type:

$$\mu_j(\phi_i) = \begin{cases} S\left(\dfrac{\overset{0\,j}{\phi_i} - \phi_i}{\varsigma_{ij}}\right), \phi_i \le \overset{0\,j}{\phi_i}, \\ Q\left(\dfrac{\phi_i - \overset{0\,j}{\phi_i}}{\underset{\varsigma_{ij}}{\xi}}\right), \phi_i > \overset{0\,j}{\phi_i}, \end{cases} \qquad (2)$$

where: S and Q arbitrary functions that do not grow on the set of positive real numbers, $\varsigma > 0$, $\xi > 0$ (Options ς and ξ are respectively the left and right fuzziness coefficients);

Membership function in terms of (S-Q) correlation functions will be described

$$\mu(\phi) = \begin{cases} \dfrac{1}{1 + \left(\dfrac{\alpha - \phi}{\beta}\right)^2}, & \phi \le \alpha, \\ \dfrac{1}{1 + \left(\dfrac{\phi - \alpha}{\beta}\right)^2}, & \phi > \alpha. \end{cases} \qquad (3)$$

FIRE consists of the three types of components: network data collector (NDC), network data processor (NDP), Fuzzy Threat Analyzer (FTA). The network data collector (NDC) is a promiscuous network data sniffer and recorder. It reads raw network packets off the wire and stores them on disk. The next component, the network data processor (NDP), summarizes and tabulates the raw packet data in carefully selected categories. In a sense, an NDP performs a kind of data mining on the collected packets. The NDP merges these summaries and tables with past data and stores them on disk. Next, the NDP compares the current data with the historical mined data to create values that reflect how the new data differs from what was observed in the past. These values are "fuzzified" to produce the fuzzy inputs needed by the Fuzzy Threat Analyzer (FTA). The resulting fuzzy inputs from the NDPs are called "fuzzy alerts" because they represent an alert condition to a degree.

Example list of factors that affect the productivity of information systems under the threat of DDoS attacks, presented in the form of linguistic variables, for which the selected set and universal terms. According constructed fuzzy knowledge base, representing a set of fuzzy rules "IF-THEN" that define the relationship between input and output variables. For fuzzy knowledge bases composed logical equation.

$$\mu^{d_j}(D) = \bigvee_{p=1}^{h_j}\left[\mu^{y_3^{jp}}(y_3) \wedge \mu^{y_4^{jp}}(y_4) \wedge \ldots \wedge \mu^{\phi_z^{jp}}(\phi_z)\right],$$

$$p = \overline{1, h_j}\,, j = \overline{1, U} \qquad (4)$$

Once the NDP completes the data mining phase, it produces fuzzy sets based on past input data. FIRE uses the historical and statistical data for each element of matrix (5) [Lahno V., A. Petrov A., 2011]. We have arbitrarily chosen five fuzzy sets for each data element: *low*, *medium-low*, *medium, medium-high*, and *high* (table 1). By standardizing the number of sets, we can apply the same fuzzy rules against the data from each NDP, regardless of the differences in the local input domain.

$$H = \begin{pmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1i} & \cdots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{2i} & \cdots & \phi_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \phi_{l1} & \phi_{l2} & \cdots & \phi_{li} & \cdots & \phi_{ln} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \phi_{N1} & \phi_{N2} & \cdots & \phi_{Ni} & \cdots & \phi_{Nn} \end{pmatrix}. \qquad (5)$$

In a common intrusion scenario, an attacker conducts a port scan of a network, sending packets to several well-known ports (FTP, HTTP, etc.) looking for systems that might be running those services. The presence of those services on a system gives a hint as to what vulnerabilities the attacker might try to exploit to penetrate the system. Additionally, the attacker may use scanners that can accurately identify the operating system on the target machine by examining the response of the TCP stack to carefully crafted TCP control messages. Knowledge of the services running and the host operating system is extremely valuable to the attacker because it helps to narrow the types of vulnerabilities the attacker can exploit on the systems. Port and operating system detection scanning may be a strong indicator that a more serious attack may be occurring in the future.

With the fuzzy input sets defined, the security administrator can then construct the rules of the fuzzy system. Fuzzy rules are written using common sense experiences by the security administrator. The rules designer seeks to define rules that cover as much of the input space as possible Using tools such as the Matlab Fuzzy Toolbox, the designer can check the input rule space to ensure that the fuzzy rules cover the input space and that all output responses are defined, figure 1.

Table 1. Factors affecting the productivity of information systems for DDoS and DoS attacks

A partial state variable of the information system and Network	**Universum**	Terms for linguistic assessment
ϕ_1 – indicator of current risks [10]	[0,1], arbitrary units (A.U.).	*low*, *medium-low*, *medium*, *medium-high*, and *high*
ϕ_2 – acceptable level of risk information	[0,1], A.U.	-
ϕ_3 – intensity of flow rate (requests) coming to servers	[10,6000], frame / s	-
ϕ_4 – nominal capacity of the environment data	[10,100], Mbit / s	-
ϕ_5 – number of attempts to access to environmental data generated by an attacker to view	$[0, \mathrm{N}_a]$	-
ϕ_6 – the service transaction	[0,001-0,01], s	-
ϕ_7 – IP pcket length	[1 -65529], byte	-
ϕ_8 – large number of IP packets with the type of attack Ping of Death	[0,1], A.U.	-
ϕ_9 – number of http-requests to the object of attack	[0,1], A.U.	-
ϕ_{10} – presence of TCP packets	[0,1], A.U.	-
ϕ_{11} – presence of UDP packets	[0,1], A.U.	-
ϕ_{12} – presence of ICMP packets	[0,1], A.U.	-
ϕ_{13} – availability of SQL injection	[0,1], A.U.	-
ϕ_{14} - interval between frames	[10-100], bit	-
…		-
ϕ_z - other factors		-

This algorithm was implemented in Delphi. Fig. 2 shows a general view of the application. We have implemented the graphs attack in a combination of Prolog and Delphi, fig. 2. Experimental results show that our logical attack graph tool is very efficient and can handle networks with thousands of machines.

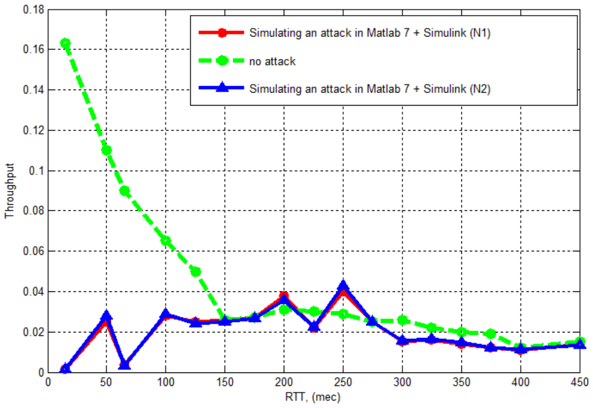
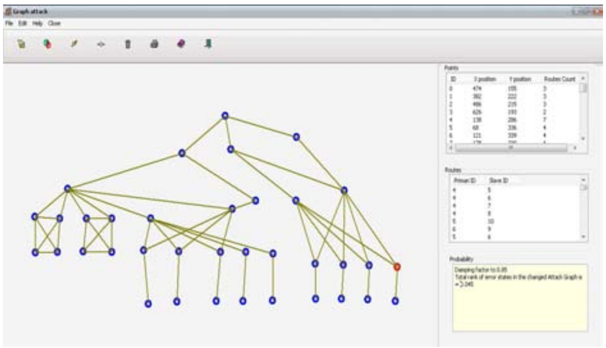


Fig 1. Dos Inter-burst Period



Points

ID	X position	Y position	Routes Count
0	474	155	3
1	382	222	3
2	486	235	3
3	628	193	2
4	138	206	7
5	68	336	4
6	121	339	4

Routes

Primari ID	Slave ID
4	5
4	6
4	7
4	8
5	10
6	9
5	8

Probability

Damping Factor to 0.85
Total rank of error states in the changed Attack Graph is =3.245

Fig. 2. Comparison in Delphi Network Attack Graphs

We show screenshots of a few examples of Network Attack Graphs. States in the graph have been ranked according to the ranking algorithm based on PageRank. We set the damping factor to 0.85. For each error state, the intensity of color is proportional to the relative rank of that state in the Attack Graph. The security metric based on the total rank of error states is a quantitative guide for comparing Attack Graphs. A system administrator could fix a particular security property, make changes to his network configuration and compare the Attack Graphs obtained using this security metric. Thus, he can determine the relative utility of different security measures. He could also fix the system model and observe changes in the ranks of the Attack Graph based on varying the security property from a weak to a strong one.

CONCLUSIONS

Hence, the applicability of the autonomous and profound research of the issues of designing new mathematical models for the estimation of the automated data processing systems (ADPS) security is conditioned by the following factors:

- obviousness and operativeness of making multialternative solutions on the ADPS security;

- presence of possibilities to check the semantic relations and ADPS compatibility, data protection facilities and attack countering;

- variety of forms and methods of detailed evaluation of attack graphs (scenarios) on ADPS and countering to them;

- imbedded facilities of the a priori processing of subject and object «roles» in the future processes of ADPS functioning under attacks.

However the practical utilization of the offered mathematical attack models requires solution of the issues of designing the sophisticated mathematical software for prevention of attack scenarios, and also developing the science-intensive program-, information - and communication facilities.

REFERENCES

1. **Ahmad D., Dubrovskiy A., Flinn X., 2005.:** Defense from the hackers of corporate networks. Trudged. with angl. - 2th izd. M.: Companies AyTi; DMK - Press. 864 p.
2. **Atighetchi M., Pal P., Webber F., Schantz R., Jones C., Loyall J., 2004.:** Adaptive Cyberdefense for Survival and Intrusion Tolerance // Internet Computing. Vol. 8, No.6. p.25-33.
3. **Atighetchi M., Pal P.P., Jones C.C., Rubel P., Schantz R.E., Loyall J.P., Zinky J.A., 2003.:** Building Auto-Adaptive Distributed Applications: The QuO-APOD Experience // Proceedings of 3rd International Workshop Distributed Auto-adaptive and Reconfigurable Systems (DARES). Providence, Rhode Island, USA. p.74-84.
4. **Chapman C., Ward S., 2003.:** Project Risk Management: processes, techniques and insights. Chichester, John Wiley. Vol. 1210.
5. **Chi S., Park J., Jung K., Lee J., 2001.:** Network Security Modeling and Cyber At-tack Simulation Methodology//LNCS. Vol. 2119.
6. **Goldman R., 2002.:** A Stochastic Model for Intrusions//LNCS. Vol. 2516.
7. **Gorodetski V., Kotenko I., 2002.:** Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool. RAID 2000//LNCS. Vol. 2516.

8. **Harel D. Statecharts: A., 1987.:** Visual Formalism for Complex Systems, Science of Computer Programming 8. p. 231-274.
9. **Hariri S., Qu G., Dharmagadda T., Ramkishore M., Raghavendra C., 2003.:** Impact Analysis of Faults and Attacks in Large-Scale Networks//IEEE Security & Privacy. p. 456-459.
10. **Hatley D., Pirbhai I., 1988.:** Strategies for Real-Time System Specification, Dorset House Publishing Co., Inc., NY. 930 p.
11. **Keromytis A., Parekh J., Gross P., Kaiser G., Misra V., Nieh J., Rubensteiny D., Stolfo S., 2003.:** A Holistic Approach to Service Survivability // Proceedings of ACM Workshop on Survivable and Self-Regenerative Systems. Fairfax, VA. p. 11-22.
12. **Lahno V., Petrov A. 2011.:** Modelling of discrete recognition and information vulnerability search procedures. TEKA. Volume XI A. p. 137-144.
13. **Lahno V., Petrov A. 2011.:** Ensuring security of automated information systems, transportation companies with the intensification of traffic: Monograph. Lugansk. 2011.
14. **Lahno V.A. Petrov A.S. 2011.:** Task The Research of the conflict Request Threads in the Data Protection Systems. Marketing and logistics problems in the management of organization. Edited by: Honorata Howaniec, Wieslaw Waszkielewicz. Chapter XV. Academia Techniczno – Humanistyczna w Bielsko-Biala. 2011. p. 230-251.
15. **Lahno V.A., Petrov A.S. 2011.:** Experimental studies of productivity change in corporate information systems for companies in terms of computer attacks. Information security № 1 (5), 2011. p.181-189.
16. **Lahno V., Petrov A., 2009.:** Prevention from Penetration into Dynamic Database of Corporate Information Systems of Enterprises. Management of Organizatoon Finances, Production, Information. Bielsko-Biala. p. 282-290.
17. **Smirniy M., Lahno V., Petrov A., 2009.:** The research of the conflict request threads in the data protection systems. Proceedings of Lugansk branch of the International Academy of Informatization. № 2(20). V 2. 2009. p. 23-30.
18. **Templeton S., Levitt K., 2000.:** A Requires/Provides Model for Computer Attacks. Proc. of the New Security Paradigms Workshop. p. 274-280.
19. **Xiang Y., Zhou W., Chowdhury M., 2004.:** A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia. p. 38-43.
20. **Slobodyanuk M., Nechaev G. 2010.:** The evaluation technique of logistics system cargo transportation efficiency development.TEKA Kom. Mot I Energ. Roln, - OL PAN, 10B. Lublin, 2010. p. 162-170.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПАНИИ ПРИ DOS (DDOS) АТАКЕ

Валерий Лахно

Аннотация. Статья содержит результаты исследований, позволяющие повысить уровень защиты автоматизированных и интеллектуальных информационных систем предприятий и компаний. В статье предложена модель системы поддержки принятия решений в случае выявления DoS (DDoS) атаки для варианта нечеткой входной информации.

Ключевые слова: информационная безопасность, атака типа отказ в обслуживании, система поддержки принятия решений.