Implementation of Communication Phase of Data Exchange Protocol Prototype between IDPSs

Oleksandra Yeremenko, Anatoliy Persikov

Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, UKRAINE, Kharkiv, Nauka Ave., 14, E-mail: oleksandra.yeremenko.ua@ieee.org, persikovanatoliy@gmail.com

Коротка анотація – У роботі пропонується варіант реалізації фази етапу обміну інформацією прототипу протоколу обміну даними між системами виявлення та протидії атакам з урахуванням таких факторів компрометації системи, як проведення екстенсивного криптоаналізу, так і вразливостей використовуваних комунікаційних технологій (компрометація елементів мережі – вузлів, каналів, маршрутів).

Ключові слова – прототип, протокол, обмін даними, система виявлення та протидії атакам, багатошляхова маршрутизація, метрика, ймовірність компрометації.

Introduction

The current problem in the deployment and operation of infocommunication networks is the provision of information security. At the same time, the use of passive means of protection, which are capable of auditing events and filtering data, does not give the desired effect, since such protection tools can not quantify the state of the network [1-4]. The main means of providing scalable active protection is the introduction of distributed Intrusion Detection and Prevention Systems (IDPSs) [5]. Therefore, an urgent task is to develop a prototype of the universal protocol of IDPS detection and data exchange between different types of IDPSs [6]. The protocol should be able to deliver data with the time and quality characteristics specified by each of the types of networks, taking into account the potential risk of data transmission via a certain communication link or a subnet.

The paper proposes an option for implementing of communication phase of data exchange protocol prototype between IDPSs taking into account such factors of system compromising as extensive cryptanalysis and vulnerabilities of the communication technologies used (compromise of network elements – nodes, links, and routes).

Realization of phases in stage of information exchange

Data exchange phase between the IDPSs (the remaining phases in this stage are used for the justified selection of the data path) can be introduced in the same way as in the OSPF protocol [7-10]. This approach provides the following options:

- limiting the distribution of information by multicasting;
- construction of an IDPS and data delivery according to the hierarchical principle;
- sending notifications immediately after the occurrence of an event (to ensure rapid network convergence and accurate assessment of information security risks);
- organization of multi-channel control system by multiple IDPSs using multipath transmitting (restricts an attacker’s view on actions of the protection system);
- rapid distributing of key information (by assigning top priority to the traffic of cryptographic keys).

The selection of the information path should be based on a certain metric. A metric (for example, similar to [7]) should also reflect the state of the communications network and take into account the risk of transmitting information along a certain path.

For the protocol, it is possible to use the modification of the EIGRP protocol metric [8]. The basic form of the metric is as follows:

$$M_{EIGRP} = \left[\left(K_1 \cdot B + \frac{K_2 \cdot B}{256 - L} + K_3 \cdot D\right)\frac{K_5}{K_4 + R}\right] \cdot 256 , (1)$$

where K_1 – K_5 are the coefficients determined by the network administrator to change the priorities for calculating the estimates (the default values are $K_1 = K_3 = 1$, $K_2 = K_4 = K_5 = 0$);

D is the route delay (accurate to tens of microseconds);

B is the minimum bandwidth of the route (in Kbps);

R is the reliability or likelihood of succesful packet transmission (the estimate is from 0 to 255, 255 is the most reliable, while 0 means no reliability);

L is the effective load of the route (the estimate from 0 to 255; 255 corresponds to 100% loading).

The EIGRP protocol calculates the scaled bandwidth and delay as:

$B = \left[10^7 / bandwidth(i)\right] \cdot 256$, where $bandwidth(i)$ is the least bandwidth of all outgoing interfaces on the route to the destination;

$D = \left[delay(i)\right] \cdot 256$, where $delay(i)$ is the sum of the delays configured on the interfaces, on the route to the destination.

Moreover, the better the parameters of the interface are, the less the value of the metric is.

The new metric should take into account two factors: the strength of the cryptographic information security system and the ability of an attacker to influence a particular network link or interface.

The first factor requires determining the probability of compromising the system P_{f1} as an indicator of inverse time (accurate to the microsecond, as defined in the EIGRP metric), which is necessary for an attacker to break a key that depends on the development of computers capable of performing parallel computations. As it is known, the statement of the updated Moore’s law that the power of advanced computers doubles every year is justified. The longer a cryptographic key is used, the more likely security system compromising will happen.

Therefore, the probability of compromising the system by performing extensive cryptanalysis P_{f_1} in the most simplified form can be defined as

$$P_{f_1} = 1 - \frac{1}{2^{t/T}}, \qquad (2)$$

where t is the time the system usage (in microseconds, to match the dimension of the delay time D);

T is the constant that indicates the number of microseconds per year and equals 31536000000000.

The preferred action when approaching the period of key usage is its change, because transiting to the increased key length can reduce the system`s resistance to attacks, as in the case of using AES [11].

The second factor is when the probability of compromising the link (subnet) of data transmission P_{f_2} is determined by information about the hardware and software platforms used. The following approach is possible to determine the indicator: the gradation of vulnerabilities according to criticality with a sharp increase in vulnerability and the subsequent choice of the minimum level of security inherent in the most unreliable (in terms of information security) element of the communication network. Even systems without identified vulnerabilities can not be considered as fully protected, because in certain circumstances, vulnerabilities can be detected by an attacker.

Therefore, the probability of compromising the system P_{f_2}, due to the vulnerabilities of the technologies used, in the most simplified form can be defined as

$$P_{f_2} = 1 - \frac{1}{K_6 \cdot n^n}, \qquad (3)$$

where K_6 is the coefficient that takes into account the possibility of compromising a potentially protected system today (use of $K_6 = 1.11$ may be recommended, which corresponds to the probability of compromising 0.1);

n is the number of the criticality index ($n = 1\mathbf{K}6$).

Since the first and second factor, in principle, can be considered as independent, the probability of compromising the system by an attacker analyzing both the first and second factors should be multiplied. Then the modified routing metric M_{SC}, taking into account the probability of system compromising, can be defined as follows:

$$M_{SC} = M_{EIGRP} \cdot K_7 \cdot P_{f_1} \cdot P_{f_2}, \qquad (4)$$

where K_7 is the coefficient that determines the computational power of supercomputers at the time of algorithm and key selection.

Conclusion

Thus, when calculating the data transmission path between IDPSs in the network, it is necessary to use the modified metric that takes into account the probability of compromising the transmission paths of information and the information itself if it is transmitted in the encrypted form. The proposed modified metric corresponds to the rule of the EIGRP metric:

- the increase of the metric under increasing computing power of supercomputers due to the decrease in the potential security of information transmission paths;
- the increase of the metric with increasing probability of compromising the transmission path due to the cryptanalysis (path selection with minimal probability of compromise);
- the increase of the metric with increasing probability of compromising the transmission path due to network vulnerabilities (choosing the path with the minimum number of potential vulnerabilities).

References

[1] Schneier, B. Data and Goliath: The hidden battles to collect your data and control your world [Text] / B. Schneier. – WW Norton & Company, 2015. – 398 p.

[2] Stallings, W. Cryptography and Network Security: Principles and Practice. 7th Edition [Text] / W. Stallings. – Pearson, 2016. – 768 p.

[3] Popovskiy, V. V. Zaschita informatsii v telekommunikatsionnyih sistemah [Text] / V.V. Popovskiy, A.V. Persikov. – Kh.: SMIT, 2006. – 238 p.

[4] Popovskiy, V. V. Osnovy kriptograficheskoy zaschityi informatsii v telekommunikatsionnyih sistemah. Vol. 1 [Text] / V.V. Popovskiy, A.V. Persikov. – Kh.: SMIT, 2010. – 350 p.

[5] NIST 800-94 Guide to intrusion detection and prevention systems (IDPS). National institute of standards and technology, 2007 – 127 p.

[6] Steinberger, J., Sperotto, A., Golling, M., Baier, H. How to Exchange Security Events? Overview and Evaluation of Formats and Protocols [Text] / J. Steinberger, A. Sperotto, M. Golling, H. Baier // 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM 2015), May 2015. – P. 261-269.

[7] De Couto, D., Aguayo, D., Bicket, J., Morris, R. A High Throughput Path Metric for Multi-Hop Wireless Routing [Text] / D. De Couto, D. Aguayo, J. Bicket, R. Morris // Wireless Networks, 11(4), 2005. – P. 419-434.

[8] Cisco Networking Academy, ed. Routing Protocols Companion Guide, 1st Edition. – Cisco Press, 2014. – 792 p.

[9] Szigeti, T. End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks. 2nd edition [Text] / T. Szigeti, C. Hattingh, R. Barton, K. Briley. – Cisco Press, 2013. – 1040 p.

[10] Lemeshko, O. Dynamic presentation of tensor model for multipath QoS-routing [Text] / O. Lemeshko, O. Yeremenko // 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2016. – P. 601–604. doi: 10.1109/tcset.2016.7452128

[11] Advanced Encryption Standard (AES). Federal Information Processing Standard Publication №197, 2001 – 51 p