Development of Data Exchange Protocol Prototype Between Intrusion Detection and Prevention Systems

Oleksandra Yeremenko, Oleksandr Lemeshko, Anatoliy Persikov
Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
oleksandra.yeremenko.ua@ieee.org, oleksandr.lemeshko@nure.ua, persikovanatoliy@gmail.com

Розробка Прототипа Протоколу Обміну Даними між Системами Виявлення та Протидії Атакам

Олександра Єременко, Олександр Лемешко, Анатолій Персіков
Кафедра інфокомунікаційної інженерії
Харківський національний університет радіоелектроніки
м. Харків, Україна
oleksandra.yeremenko.ua@ieee.org, oleksandr.lemeshko@nure.ua, persikovanatoliy@gmail.com

Abstract—**The data exchange protocol prototype between Intrusion Detection and Prevention Systems is proposed. One of the candidates for the universal protocol for managing and exchanging of information between IDPS systems is IDXP, however, it has a number of limitations. As a result there arises the task of developing a protocol that solves the issues of detecting various types of IDPSs in the network, exchanging attack signatures between IDPSs, coordinating actions to manage the state of the network and efficient information exchange in a potentially insecure network with an irregular structure. The protocol should take into account the differences in IDPS workflows and how to capture information about events in the network, the possibilities of analyzing the network state, and the functional capabilities of devices acting as data accumulating elements.**

Анотація—**Запропоновано прототип протоколу обміну даними між системами виявлення та протидії атакам. Одним з кандидатів на роль універсального протоколу для управління та обміну інформацією між IDPS системами є IDXP, проте він має ряд обмежень. Отже виникає задача розробки протоколу, який вирішує завдання проведення виявлення різних видів IDPS в мережі, обміну сигнатурами атак між IDPS, узгодження дій з управління станом мережі та ефективного обміну інформацією в потенційно незахищеній мережі з нерегулярною структурою. Протокол повинен враховувати відмінності в схемах роботи IDPS і способах фіксації інформації про події в мережі, можливості проведення аналізу стану мережі, а також функціональних здібностях пристроїв, які виступають в ролі елементів, що акумулюють дані.**

Keywords—prototype; protocol; data exchange; Intrusion Detection and Prevention System; IDXP

Ключові слова—прототип; протокол; обмін даними; система виявлення та протидії атакам; IDXP

I. Introduction

Public networks, such as the Internet, and networks integrated with it are open infocommunications, services of which are used by millions of users. Every day hundreds of thousands attempts to violate network performance in general are made. These attempts are mostly initiated by professional attackers, who possess special software tools and hardware with enormous computing power [1, 2].

That is why a relevant problem of such a type of networks is to provide information security (IS), which means realization of different procedures and tasks: authentication, identification, authorization, audit, confidentiality and integrity of information, etc. [2, 3]. In general, attack prevention in a single segment of a large or small network has no sense because networks based on packet-switching technology and IP protocol are fault-tolerant due to the possibility of selecting a set of information transmission routes [4-8]. That is why the attacker is able to avoid secure segments and spread his actions at vulnerable ones [1-3].

Implementation of passive protective means able to perform auditing of events and data filtering does not give the necessary effect, because such protective means cannot provide quantitative evaluation of the network state [3]. In modern security systems the emphasis should be done on using active means of security able to accumulate data on different events in the network, to conduct multi-criteria analysis of these data and influence the state of network elements with the help of common or specific interfaces [3] (i.e. to perform active auditing).

The major means for providing active scalable protection is introduction of distributed Intrusion Detection and Prevention Systems (IDPS) [9]. An IDPS should support real time operation to perform the following activities:

realization of protection mechanisms corresponding to the network security policy;

detecting an intrusion and forecasting of attacker`s intensions and actions;

evaluating potential vulnerabilities, data collection and analysis of the current state of the network and security system;

implementing contractions, including suppression of the attacker`s actions and redistribution of the load between the critical protection mechanisms;

reducing consequences of intrusion and identifying vulnerabilities, adapting the IS system to better counteract the already studied attacks in the future.

The drawback of modern IDPSs is the lack of effective exchange protocols that allow data exchange between IDPSs of different manufacturers [9] oriented to different formats of data storage and exchange. The protocols offered by the Internet community [10-12] do not meet all the requirements of modern security systems [1, 2]. In addition, these protocols only consider the task of universal data formatting, but they do not cover the issues of dynamic detection of IDPS elements in networks and data routing in a potentially vulnerable network.

Therefore, a relevant problem and task is the development of a prototype of the universal protocol (protocol stack) for IDPS detection and data exchange between different types of IDPS. The protocol should be able to deliver data with the time and quality characteristics given by each of the types of networks, taking into account the potential danger of data transmission over a certain link or a subnet.

II. Basic Requirements to Modern Secure Data Exchange Protocols between IDPS

Currently, there are published several exchange formats and protocols (for example, the Intrusion Detection Exchange Protocol (IDXP)) and used for the exchange of information between different IDPSs [10, 11]. Nevertheless, the IDXP protocol [12] is oriented only to the problem of universal data formatting within Intrusion Detection Message Exchange Format (IDMEF) [13]. Analysis of the capabilities of IDXP/IDMEF has shown that:

the protocol does not solve the problems of the phase of negotiations on the selected information exchange technologies (including protocols and cryptographic algorithms);

the protocol is applied and oriented to point-to-point connection, which involves the use of a service transport protocol that can be compromised before a secure connection is established;

the protocol declares the possibility of multipath data exchange, but does not describe it;

there is no implementation of the connection pooling, so there is a need to re-generate the secure connection with the subsequent transmission of messages.

However, despite these shortcomings, IDXP/IDMEF ideas can be used in the protocol prototype to solve the problems of universal data formatting.

The protocol prototype should be of the Network Layer (an approach similar to that defined in IPv6 [14] can be selected) to perform data routing and accelerated device discovery by sending frame signals about the presence of an IDPS object of a certain type [15]. Providing mutual authentication of network elements in this case can be realized by using the Extensible Authentication Protocol (EAP) [16].

To deliver messages between hosts where IDPS works, a “routed protocol – transport protocol” binding can be used. As a routed protocol, IPv4 and IPv6 can be chosen [2] (in the case of cryptographic security IPsec [17]), and as the transport protocol we can choose the BEEP-encapsulated [18] TCP protocol [19]. In principle, considering IDPS as a routing device that can monitor the state of routers in the network, one can create an overlay communication network related to the tasks of detecting and preventing attacks.

Delivery of messages describing various types of vulnerabilities and ways to counter them should be carried out using a universal data format, which is a text format. The markup of text data can be performed using a certain markup language based on the Standard Generalized Markup Language (SGML) specification [20]. Since it is assumed that the protocol prototype is compatible with IDXP, Extensible Markup Language (XML) will be selected as the markup language. For the encoding of information, the Multipurpose Internet Mail Extensions (MIME) standard [21] can be used, and in the case of cryptographic security – Secure/Multipurpose Internet Mail Extensions (S/MIME) [22]. In the case of S/MIME, encryption (optionally with compression) of transmitted messages is implemented, and therefore, Network Layer security services can be limited by mutual authentication of nodes and matching of session keys. In fact, there is no need to create a full cryptographic tunnel between hosts where IDPSs operate, which increases the system operation speed in general [23, 24]. This aspect is important when scaling the integration of IDPS systems and under simultaneous operation of tens of thousands of devices. The data request/data management can be carried out on the basis of the HTTP protocol [25], which will allow signaling in heterogeneous networks, where firewalling is used [2, 3] (since the transmission of HTTP messages is usually not blocked).

The second task (after ensuring compatibility of systems by unifying the format of data representation), which is solved when choosing a data markup language, is the task of ensuring that the network state uncertainty does not increase as new

IDPS data are received from other IDPSs. The level of uncertainty increases in the following cases:

receiving incorrect data imposed by an attacker;

receiving corrupted data that will be incorrectly interpreted;

late reception of data due to delays in the network (including those caused by the impact of attacks), untimely data transmissions, as well as the need to convert data;

obtaining correct data, however, they are presented in a different format (resulting in an increase in the total number of system states).

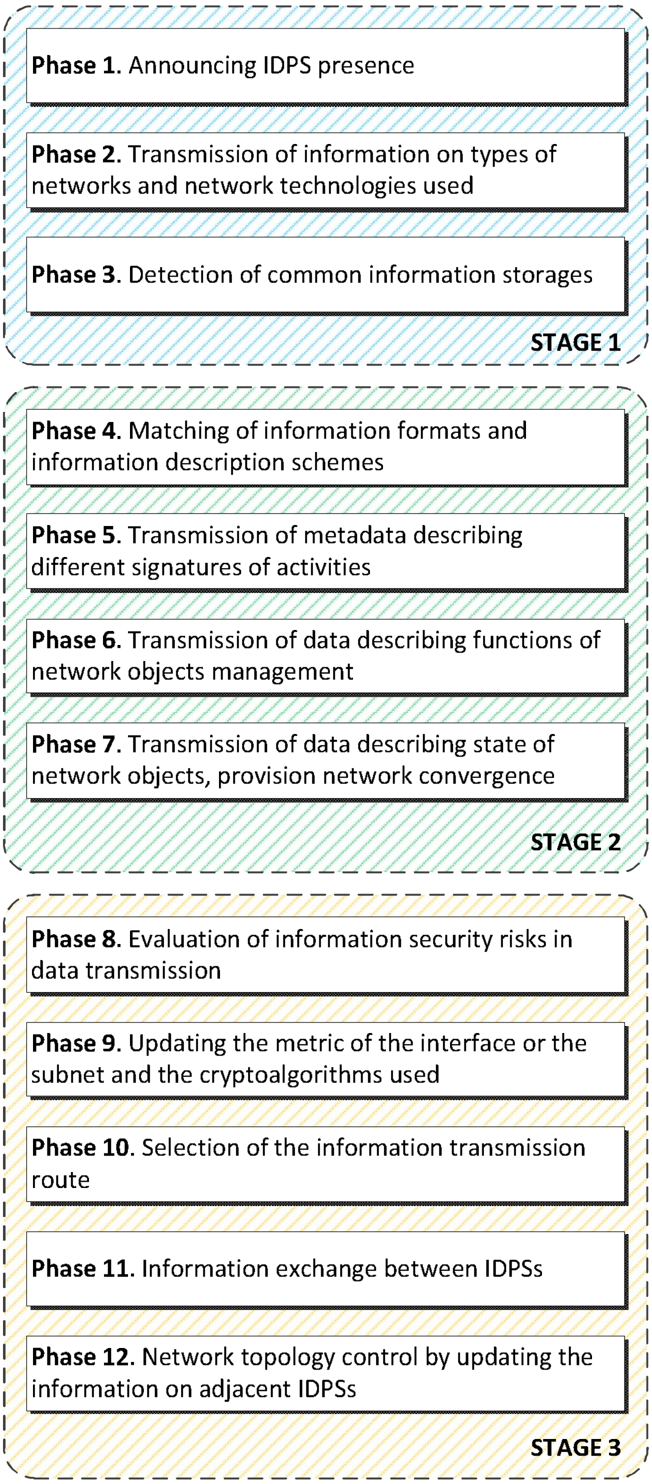
To resist the imposing of data by an attacker is possible through the use of integrity primitives [23, 24] and special MIME markup (S/MIME). Tagging markup of the XML protocol allows to detect syntax mismatches and, therefore, to identify incorrect message fragments. This will allow to avoid sending incorrect data to the analysis system (including those presented in a different format). Delayed data delivery can be avoided by using the Traffic Engineering [6, 26-28] orientation and resource reservation along the data path [4]. In the case if traffic is not delivered over a certain set of paths during the predetermined number of times, these paths must be excluded from the network topology.

III. Stages of Exchange Protocol Operation

The protocol prototype consists of three stages, each of which in turn consists of a certain number of phases (Fig. 1). The division into phases and stages is done in such a way that the actions within the stage can be performed cyclically, and the transition from one stage to the next one is possible only if all the phases of the stage are successfully completed.

Most of the phases are independent elements of the protocol and can be executed regardless of other phases. This enables parallel execution of actions within the protocol with a constant change in the presentation of the network within the integrated IDPS system. The transfer of information and network management can then be performed in an iterative manner, i.e. management will be improved as more information becomes available.

The emphasis in the exchange protocol within the IDPS system should be made on ensuring that the representation of the network state cannot be deteriorated and that only the relevant information, which is not imposed by the attacker, is received.



Phase 1. Announcing IDPS presence

Phase 2. Transmission of information on types of networks and network technologies used

Phase 3. Detection of common information storages

STAGE 1

Phase 4. Matching of information formats and information description schemes

Phase 5. Transmission of metadata describing different signatures of activities

Phase 6. Transmission of data describing functions of network objects management

Phase 7. Transmission of data describing state of network objects, provision network convergence

STAGE 2

Phase 8. Evaluation of information security risks in data transmission

Phase 9. Updating the metric of the interface or the subnet and the cryptoalgorithms used

Phase 10. Selection of the information transmission route

Phase 11. Information exchange between IDPSs

Phase 12. Network topology control by updating the information on adjacent IDPSs

STAGE 3

Fig. 1. Tasks supported by the data exchange protocol.

IV. Conclusion

One of the candidates for the universal protocol for managing and exchanging of information between IDPS systems is IDXP, however, it has a number of limitations. That is why there arises the task of developing a protocol (protocol stack) that solves the issues of detecting various types of IDPSs in the network, exchanging attack signatures between IDPSs, coordinating actions to manage the state of the network and efficient information exchange in a potentially insecure network with an irregular structure. The protocol should take into account the differences in IDPS workflows and how to capture information about events in the network, the possibilities of analyzing the network state, and the functional capabilities of devices acting as data accumulating elements.

When calculating the data route between IDPSs in the network, it is necessary to use a modified metric that takes into account the probability of compromising the information transmission route and the information itself if it is transmitted in the encrypted form. In further development the modified metric is proposed to use, which corresponds to the rule of the Enhanced Interior Gateway Routing Protocol (EIGRP) metric:

as the computing power of supercomputers increases, the metric increases, i.e. the potential security of the information route decreases;

when the probability of compromising the path is increased due to cryptanalysis, the value of the metric increases, i.e. the path will be chosen, where the probability of compromise is minimal;

when the probability of compromising the path is increased due to the vulnerabilities of the communication network, the value of the metric is increased, i.e. the path will be chosen where the number of potential vulnerabilities is minimal.

It should be noted that in this paper we propose only a prototype of the protocol and examine the main provisions that need to be met when developing a real protocol. Therefore, further work in this direction should expand and generalize the provisions of the prototype protocol.

REFERENCES

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

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

[3] V.V. Popovskiy, and A.V. Persikov, “Zaschita informatsii v telekommunikatsionnyih sistemah,” OOO “Kompaniya SMIT”, 2006, 238 p.

[4] M. Barreiros, and P. Lundqvist, “QOS-Enabled Networks: Tools and Foundations,” Wiley Series on Communications Networking & Distributed Systems, 2nd Edition, Wiley, 2016, 254 p.

[5] I. Chen, A. Lindem, and R. Atkinson, “OSPFv3 over IPv4 for IPv6 Transition RFC 7949,” IETF, Aug. 2016.

[6] O.V. Lemeshko, O.S. Yeremenko, N. Tariki, and A.M. Hailan, “Fault-Tolerance Improvement for Core and Edge of IP Network,” XIth International Scientific and Technical Conference Computer Science and Information Technology (CSIT`2016). Conference Proceedings, Lviv, Ukraine, pp. 161-164, September 6-10, 2016.

[7] T. Szigeti, C. Hattingh, R. Barton, and K. Briley, “End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks,” 2nd Edition, Cisco Press, 2013, 1040 p.

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

[9] K. Scarfone, P. Mell, “Guide to intrusion detection and prevention systems (IDPS),” NIST special publication, Feb. 2007, 800(2007):94.

[10] J. Steinberger, A. Sperotto, M. Golling, H. Baier, “How to Exchange Security Events? Overview and Evaluation of Formats and Protocols,” 2015 IFIP/IEEE InternationalSymposium on Integrated Network Management (IM 2015), May 2015.

[11] R. Danyliw, J. Meijer, and Y. Demchenko, “The Incident Object Description Exchange Format RFC 5070 (Proposed Standard),” IETF, Dec. 2007.

[12] B. Feinstein, and G. Matthews, “The Intrusion Detection Exchange Protocol (IDXP),” RFC 4767 (Experimental), IETF, Mar. 2007.

[13] H. Debar, D. Curry, and B. Feinstein, “The Intrusion Detection Message Exchange Format (IDMEF) RFC 4765 (Experimental),” IETF, Mar. 2007.

[14] J. Bound, Y. Pouffary, S. Klynsma, T. Chown, and D. Green, “Ipv6 Enterprise Network Analysis-IP Layer 3 Focus RFC 4852”, April 2007.

[15] T. Narten, W.A. Simpson, E. Nordmark, and H. Soliman, “Neighbor discovery for IP version 6 (IPv6) RFC 4861,” IETF, Sept. 2007.

[16] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, “Extensible authentication protocol (EAP) RFC 3748,” IETF, June 2004.

[17] S. Frankel, and S. Krishnan, “IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap RFC 6071,” IETF, Feb. 2011.

[18] M. Rose, “The Blocks Extensible Exchange Protocol Core,” RFC 3080 (Proposed Standard), IETF, Mar. 2001.

[19] M. Rose, “Mapping the BEEP core onto TCP RFC 3081,” IETF, Mar. 2001.

[20] Standard, S.G.M.L., Information processing – Text and Office Systems – Standard Generalized Markup Language (SGML). First edition, ISO 8879:1986(E), [Geneva]: International Organization for Standardization, 1986-10-15.

[21] N. Freed and N. Borenstein, “Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,” RFC 2045 (Draft Standard), IETF, Nov. 1996.

[22] B. Ramsdell, and S. Turner, “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification RFC 5751,” IETF, Jan. 2010.

[23] V.V. Popovskiy, and A.V. Persikov, “Osnovy kriptograficheskoy zaschityi informatsii v telekommunikatsionnyih sistemah,” Ch. 1, Kharkiv, Kompaniya SMIT, 2010, 350 p.

[24] V.V. Popovskiy, and A.V. Persikov, “Osnovy kriptograficheskoy zaschityi informatsii v telekommunikatsionnyih sistemah,” Ch. 2, Kharkiv, Kompaniya SMIT, 2010, 294 p.

[25] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, “Hypertext transfer protocol--HTTP/1.1 RFC 2616,” IETF, June 1999.

[26] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao, “Overview and Principles of Internet Traffic Engineering RFC 3272, IETF, May 2002.

[27] Y. Lee, Y. Seok, Y. Choi, and C. Kim, “A Constrained Multipath Traffic Engineering Scheme for MPLS Networks,” Proc. IEEE ICC’2002, Publisher: IEEE, New York, pp. 2431-2436, May 2002.

[28] Al-shawi, M., and Laurent, A, “Designing for Cisco Network Service Architectures (ARCH): Foundation Learning Guide,” 4th Edition, Cisco press, 2017, 944 p.