BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 68, No. 2, 2020
DOI: 10.24425/bpasts.2020.131846

Authentication over Internet Protocol

Ł. APIECIONEK[1]*, J.M. CZERNIAK[1], M. ROMANTOWSKI[1], D. EWALD[1], B. TSIZH[2], H. ZARZYCKI[3], and W.T. DOBROSIELSKI[1]

[1] Institute of Technology, Department of Computer Science, Kazimierz Wielki University, Poland
[2] Prof. Stepan Gzhytsky National University of Veterinary Medicine and Biotechnologies Lviv, Ukraine
[3] University of Information Technology and Managment Copernicus, ul. Inowrocławska 56, 53-648 Wrocław, Poland

Abstract. Defending against DoS (denial of service) attacks has become a great challenge, especially for institutions that provide access to their services in the public network. State-of-the-art identity concealing tools and vast number of computers connected to the network require ensuring appropriate means for entities at risk to enable defence from the particular type of threats. This article presents a concept of user authentication in IP communication. The concept consists in providing the receiver with the possibility to determine sender's identity at the Internet layer level. This provides both the capability of defence against DoS attacks and possibility of utilizing the presented model over existing Internet network, which is directly responsible for transmission. The authors hope that the concept is a significant step in the perception of public network data transmission.

Key words: network security, communication, Internet Protocol, DoS attacks.

1. Introduction

Initially, when the communication model was still under development, information leakage and appropriate ways of transmitted data ciphering were considered. At present, the model [1] should be extended with one additional element – i.e. the enemy attacker (Fig. 1), whose aim is to put the system infrastructure out of operation, which results in obstructing the access to the system data and services.

1.1. Denial of service (DoS) attacks. Nowadays the number of attacks against computer systems by no means could be regarded as occasional. The industry espionage, patent theft and locking web pages has become common practice [2]. A large number of new technologies require new protection methods [3]; this applies in particular to critical infrastructures [4]. Professional literature presents a wide variety of means and methods of performing DoS attacks, such as TCP SYN, RST, ICMP, DNS or flooding. The ways of such sort of attack detection and prevention (i.e. trough packet filtering) are also frequently discussed. It is evident that systems ought to be secured against attacks and, should attacks happen, their source ought to be detected and identified [5–7]. Nevertheless, implementing security algorithms and proving their effectiveness is a problematic, which is often raised by the authors of such concepts. Moreover, additional authorisation methods, implemented on multilevel basis, may improve the security, but also cause new problems by expanding the number of components prone to overload [8].

There are various means of fighting DoS attacks and numerous algorithms and defense concepts have been proposed, such as communicating host address space inspection [2], particular algorithms of providing access to resources [9], applying marking packets, in order to determine the attack source [10, 11], utilizing firewalls that mediate the TCP transmission as well as active network monitors [6]. Common approach in computer systems is a layered structure that may be used in preventing DoS attacks as well. A similar approach is also applied in the user authentication method that is presented in this article in detail.

*e-mail: lapiecionek@ukw.edu.pl

Manuscript submitted 2019-06-27, revised 2019-08-26, initially accepted for publication 2019-10-13, published in April 2020

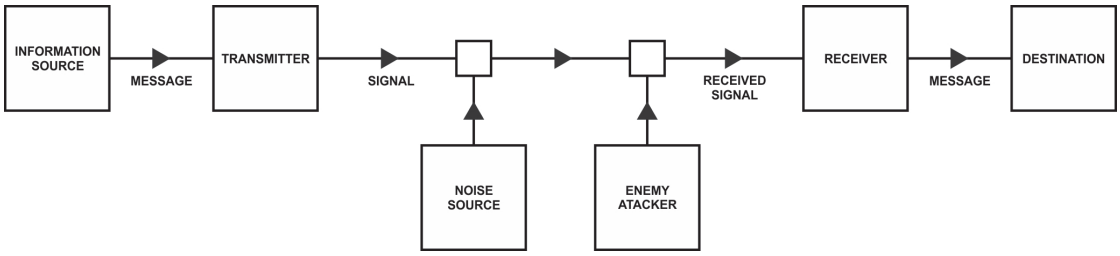

Fig. 1. Computer systems communication model

1.2. The purpose of this paper. The authors' goal is to elaborate a method that significantly reduces the risk of disrupting or obstructing the communication caused by the DoS attack. The fundamental assumption is to achieve the capability of applying the method to systems that are available over the public network (such as banking systems, or web pages of governmental institutions), with finite system resources and (almost) unlimited attacker resources. In addition, it was assumed, that the implementation of the method should provide the ability to communicate simultaneously through secured and "ordinary" channel. The first way may be utilized by privileged individuals (such as institution customers or employees), while the second one is intended to be used by other users.

The second assumption is to focus on creating the "a priori" protection which would hinder the attack possibility, rather than on attack analysis and reducing the risk "a posteriori". This explains why the authors concentrate in the paper on existing authentication and authorization methods instead of methods of fighting DoS attacks.

The third essential assumption is to provide the possibility to apply the method while utilizing the Internet (based on IPv4), with no need to modify existing systems (such as applications, web sites etc.). It was also assumed that the user would be identified by a token, that may be ensured based on various user identification methods (such as smart cards, elec-tronic IDs, biometric data, credentials, or other). The token may be assigned to the user either permanently or for a fixed period of time. What is more, it was assumed that the token would be delivered to the user with other communication channel (than protected one). In the example, the user can receive a smart card by mail or personally, which is similar to delivering credit cards or token generators for banking systems. The temporary token may be delivered by SMS.

This paper presents a general concept of transmission authentication for packet-based communication and its application in IP communication. Section 2 describes currently applied authentication and authorization models. Section 3 presents the user authentication method at transmission level, firstly for general packet transmission, and secondly for the IP packets. Section 4 focuses on the method application properties and capabilities, its advantages and disadvantages. This method is presented according to IPv4, but can also be implemented in IPv6.

2. Related work

The efficiency of attacks on computer systems which occurred after the ACTA international agreement was signed has unveiled the weakness of computer systems in fighting DoS attacks and thus the necessity to devise new methods of securing access to key resources of enterprise, institution and governmental agencies.

2.1. Existing approaches. There is a variety of authentication and authorization mechanisms currently in use. An authenticated user is deprived of his anonymity, and the organization which verified them gains confidence that the user is the person they claim to be. The Kerberos, NTLM and IPSec are the most often applied methods and protocols. It should be pointed out that they are utilized for different purposes, therefore they should not be compared directly. Nevertheless, for the authors of this paper they constitute a certain point of reference for the innovative approach of this study.

2.1.1. Kerberos. Kerberos has been developed at the Massachusetts Institute of Technology [12, 13]. It is a protocol designed for the purpose of user authentication. The operation principle of this method consists in utilizing a key distribution center (KDC), which includes an authentication server and a token generation server. The user is required to perform an authentication at KDC and gain a connection token before connecting to the target service. The user authentication can be performed by one of diverse existing tools [14, 15]. Strong encryption protocols enable users to be identified even in public networks [16]. The shortcoming of this method is that clients are authenticated on a single server. Even though it is possible to deploy the authentication server on multiple physical devices, it still requires high performance infrastructure while operating with a large group of users. Moreover, the

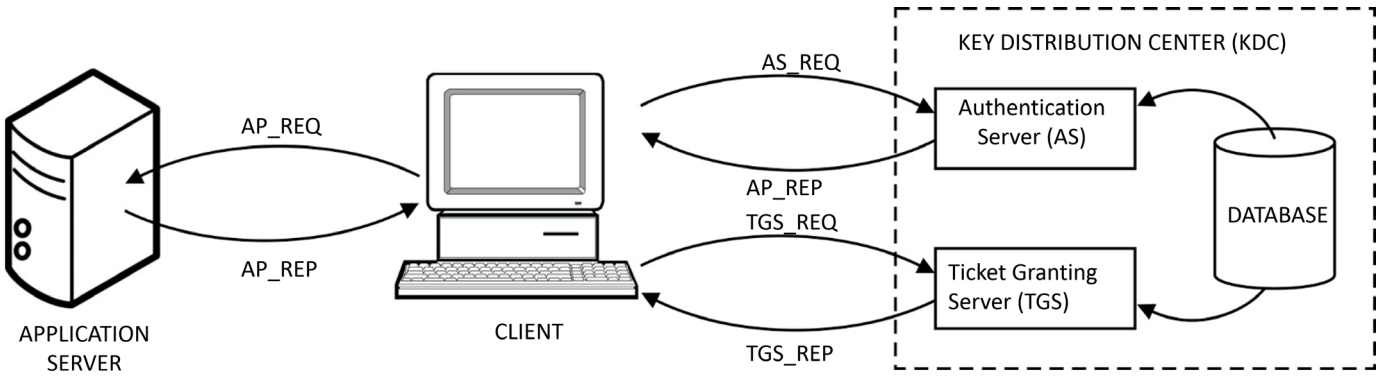

Fig. 2. Architecture of system with applied Kerberos authentication [19]

method is vulnerable to DoS attacks, since a successful attack on authentication server puts the entire system out of operation. In addition, the application of the method requires specific implementation of services which, in many cases, may be a serious obstacle [17, 18].

2.1.2. NTLM is an authentication protocol developed by Microsoft Corporation [20]. This method requires a login, domain and password hash in order to authenticate the user. The protocol may also be applied in local environment by standalone computers.

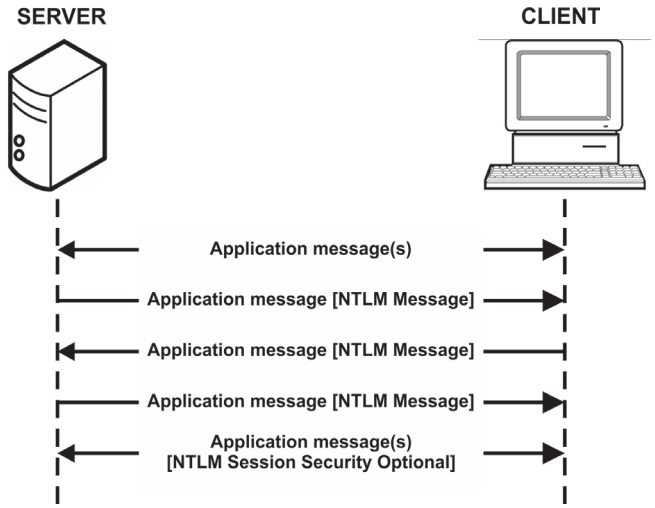

Fig. 3. Typical NTLM protocol authentication

The component responsible for authentication is a server called domain controller that stores user information.

The drawback of this method is that password hash interception allows access without knowing the actual password. For this reason Microsoft implemented Kerberos to its services.

2.1.3. IPSec. The IPSec protocol suite contains methods of safe connection to internal network (building a private tunnel called virtual private network). IPSec provides authentication, data integrity and authenticity, and encryption. Protocols that are utilized provide user authorization and data encryption [21–23]. The ESP (encapsulating security payload) protocol is designed for data source authentication. IKE (Internet key exchange) protocol provides user authentication and encryption keys exchange. AH (authentication header) protocol secures authentication and integrity at the IP packet level. The IPSec is a set of sophisticated tools. The advantage is user authentication and data encryption capability. Users may be authenticated using pre-shared keys, RSA keys and digital certificates. Regardless of authentication protocol (ESP or AH) the IPSec attaches its own header to IP packets.

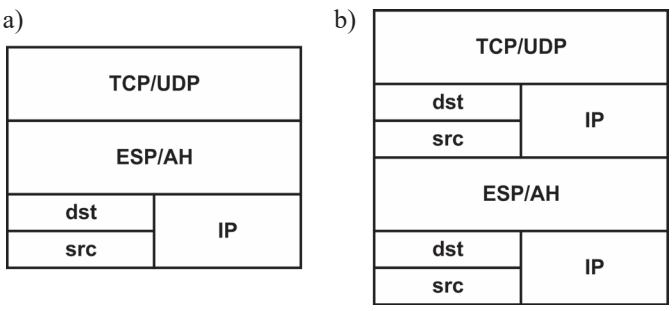

Fig. 4. Packet format a) transport mode, b) tunel mode

The IPSec drawback is that it requires data encryption resulting in the need for high performance of the device that utilizes it. This results in either reducing network transmission throughput or transmission delays. The protocols are quite resistant to attacks. The level of security depends on the selected type of user authentication – shared password or digital certificates.

2.1.4. WireGuard. Donenfeld proposed WireGuard [24, 25] as a replacement for existing secure communications protocols such as IPsec. It is high performance as regards software, and has small codebase, as the protocol is implemented in less than 4,000 lines of code, but excluding crypto primitives. It is also highly modular, provided with a key exchange phase, called the handshake, which is presented as being clearly separated from the subsequent use of the keys in a data transport protocol. A key feature is the one-round (or 1-RTT) nature of the key exchange phase. It includes an option of using pre-shared keys. The key exchange phase relies on the BLAKE2s hash function for hashing parts of the transcript to build HMAC (a hash-based MAC algorithm), and for HKDF (an HMAC-based key derivation function). The data transport protocol uses solely ChaCha20-Poly1305 as specified in RFC 7539 as an AEAD scheme in a lightweight packet format. The AEAD processing incorporates explicit sequence numbers and the receiver uses a standard sliding window technique to deal with packet delays and reordering. The inventors of WireGuard declare that with this solution it is possible to achieve better network throughput using the same security as IPSec. However, there have been tests in which WireGuard users could not achieve such results as WireGuard authors [13].

2.2. Summary. Although the methods presented above are widely used, they do not meet the assumptions established for this study. Above all, none of them is adjusted to a large user group usage, due to high hardware requirements and complex connection configuration. What is more, they are not resistant to attacks performed from public network with vast number of resources (for example attack on Kerberos authentication server possibility, NTLM password hash interception risk and high hardware requirements of IPSec). Additionally, the IP-Sec is based on connection encryption, which in some cases is redundant (commonly used HTTP protocol does not provide encryption, the HTTPs executes encryption at the application layer). There are of course other solutions such as OpenVPN or TunSafe, but they will be compared in the next study and publication.

With regard to the conclusions presented above, it is considered reasonable to devise a new concept of user authentication at connection level.

3. Authentication over IP (AOIP)

This chapter describes the concept of transmission authentication in packet based communication. Subsequently, the application of the concept in IP protocol is presented.

3.1. A general idea for packet based communication. Let M be a message that is send from a sender to a receiver using packet based transmission. In accordance with the communication protocol, the message is split into n packets, where each packet is marked as v. It should be noticed that $n \geq 1$.

3.1.1. The transmission packet. The packet v may be defined as $\{v_H, v_D\}$ where v_H is a packet header, whereas v_D stands for packet data. The function F_{MV}, that divides message M into packets, is defined as $V = F_{MV}(M)$. The $V = \{v_1, v_2, \ldots, v_n\}$ is a vector of n packets. There is an inverse of F_{MV} function F_{MV}^{-1}, defined as $M = F_{MV}^{-1}(V)$. Therefore, before message M is actually sent, it is transformed into V by the transmission channel (F_{MV}). Similarly, the receiver transmission channel reconstructs M on the basis of V $V\left(F_{MV}^{-1}\right)$.

3.1.2. The authenticated packet. The packet v_A, called the authenticated packet, which contains authenti-cation data, is defined as follows: $v_A = \{v_H, a_E, v_D\}$, where a_E is a partially encrypted authentication segment (a) of v_A. The value of a is defined as $a = \{r, t, c\}$. The quantities r, t and ch are described below. A unique number r of packet v_A is a number that, in a certain time, will be unique for each packet and each message M dispatched by every sender. This number prevents an attack performed by repeatedly sent intercepted packet.

The token t of the user u is a value of function $f_T(u)$. f_T is a function that assigns a unique token value to each user from the set of users U. It should be mentioned that f_T is an injective, has value for each element of the U set, and it should also have an inverse function $fT - 1$, such that $f_T^{-1}(t) = u \Leftrightarrow f_T(u) = t$. The quantity t is used to identify the sender.

A checksum c of packet data v_D is a value of the function $f_C(v_D)$. The function f_C is a function, for which

- $\forall v_{D1} \neq v_{D2} P\left[f_C(v_{D1}) = f_C(v_{D2})\right] \sim 0$.

The quantity c assures the data integrity. It prevents a potential attack by inserting an intercepted authentication header into another packet than the original one.

Let f_A be such a function that:

- $v_A = f_A(v)$ and
- $v = f_A^{-1}(v_A)$.

Then a vector $V_A = \{v_{A1}, v_{A2}, \ldots, v_{Am}\}$, where $m \geq n \geq 1$, is a vector of authenticated packets. One can define a pair of functions F_A and F_A^{-1} where:

- $V_A = F_A(V)$ and
- $V = F_A^{-1}(V_A)$.

In order to send a message M with authenticated packets, the transmitter performs the following operation:

- $V_A = F_A\left(F_{MV}(M)\right)$.

The message reconstruction at the receiver is as follows:

- $M = F_{MV}^{-1}\left(F_A^{-1}(V_A)\right)$.

3.1.3. Packet filtering. Let f_S be a selection function which returns a value of 1 for a valid authenticated packet v_A, and for the incorrect one it returns 0. The packet validity is approved when it the meets the following conditions:

1. For a token t enclosed in packet v_A:
   - $\exists u \in U f_T^{-1}(t) = u$,
2. A checksum c contained in packet v_A is equal to checksum of v_D:
   - $f_C(v_D) = c$,
3. The number r occurred during absence of transmission from any user in certain time.
   Let the F_S function be defined as:
   - $F_S(V_A) = V_A$ if $\forall v_A \in V_A f_S(v_A) = 1$, otherwise
   - $F_S(V_A) = V_0$, where the V_0 is an empty packet vector.

Receiving filtered messages can be noted as:

- $M = F_{MV}^{-1}\left(F_A^{-1}\left(F_S(V_A)\right)\right)$

3.1.4. Packet selection. As per the assumptions, it is possible to communicate simultaneously using both authenticated packets and packets without authentication. A choice function $f_D(v_I)$ is required in order to distinguish the type of the packet. For each incoming packet v_I the function returns 1 in case the packet is authenticated, otherwise it returns 0.

3.1.5. Summary. The concept presented above is a general idea which can be applied in many communication protocols based on packet transmission. The functions F_A^{-1}, F_S and f_D that were introduced do not affect the communication between the sender and the receiver, but add an intermediate layer.

The following part of this chapter describes implementation of this general idea to the IP protocol.

3.2. Application of the concept to Internet Protocol. The IP is a communication protocol classified as a network layer according to OSI model. The protocol has been standardized with RFC 791 [21] document. It uses a packet as a transmission entity.

This part of the chapter provides the description of application scenarios. What is more, the authenticated IP packet structure is presented in detail.

The AoIP method allows services to be accessible in public networks, having the system secured from DoS attacks by introducing the capability of IP packet authentication at the level of a device that protects the internal network. The publicly available servers may only be reached through network gateway – i.e. a firewall. This is related to opening specific ports for connection to the server out of the public network. Vast number of connections or large traffic may result in server overload and its non-responding. The AoIP method application enables marking of each packet at its source – the an external user. Packets are identified at the firewall.

Firewall devices usually have higher capability of controlling the packet transport than target service servers. The user trying to connect to the service server uses the AoIP mechanisms to mark the packets. The firewall validates packets (f_S) and transmits them to the destination. Packets with no authentication elements are dropped.

The algorithm can be described as follows:

1. The IP packet (v_I) reaches the firewall device.
2. Firewall processes the v_I packet using distinguishing function f_D.
3. If v_I is an authenticated packet (v_A), it is validated using f_S function. In case the validation is positive, the packet is transmitted to the destination server, otherwise it is dropped.
4. If v_I is an ordinary packet (v) it is dropped.

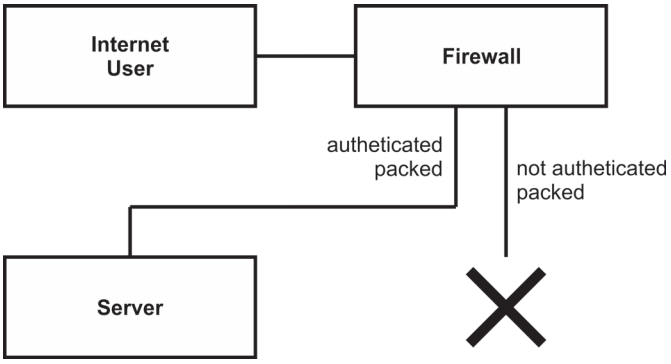

Fig. 5. Operating scheme of network with AoIP service

The above solution requires the popularization of AoIP. The following new firewall device features have to be introduced:

- ability to block unauthorized packets,
- ability to pass a specific (configurable) number of unauthorized packets to the destination,
- capability to automatically adjust the maximum number of unauthorized packets that may be passed to the destination server.

The basic diagram of AoIP application in a firewall device was presented above. However, there are extended features available for combining the firewall and the specific router, which may enable:

- adjustment of additional priorities for different groups of users (i.e. key partners, employees or customers),
- applying additional servers to adjust the traffic and resource load.

The parallel server deployment techniques are currently developed and utilized [26]. It should be pointed out that AoIP method may enhance those features by means of its specific load balancing data. This would enable the high priority group to make use of a specific server, while the low priority group uses another one. The choice, based on processing AoIP header, extends the capabilities of mechanisms that assure operation continuity. One of the routers, which are easy to be adapted to such tasks, is a VyOS software [27] available as an open source

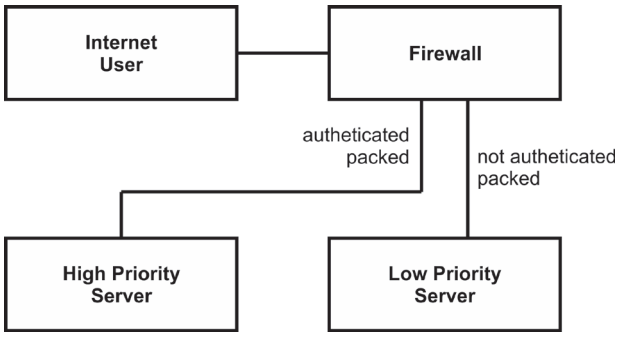

Fig. 6. Operating sheme of network with AoIP service and user priorities

package. This fact is intended to be used for future research of the AoIP concept. The algorithm extended with user priorities can be specified as follows:

1. The IP packet (v_I) reaches the firewall device.
2. Firewall processes the v_I packet using distinguishing function f_D.
3. If v_I is an authenticated packet (v_A) it is validated using f_S function:
   - in case the validation outcome is positive, the packet is transmitted to the high priority destination server;
   - otherwise it is dropped.
4. If v_I is an ordinary packet (v) it is transmitted to the low priority destination server.

The following part of this section describes the structure of authenticated IP packet.

3.2.1. Authentication over IP. As it has been stated above, the AoIP protocol is an application of authenticated packets concept to the IP protocol. It extends the IP packet with additional elements. The authentication header aE is attached before the actual IP packet data segment. This modification additionally requires the altering of the TOTAL LENGTH field, while the original value should be increased by the authentication header length. The IP packet containing AoIP elements is presented in Fig. 7.

It should be mentioned that extending the data segment of IP packet may result in exceeding the maximum packet size. In this case, the packet should be fragmented according to IP protocol specification.

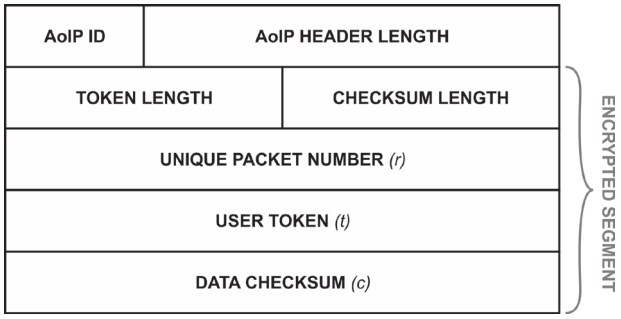

Fig. 7. IPv4 packet structure with AoIP elements

The authentication header for IP packet (AoIP header in short) consists of the following elements:

1. *ID*, that is an AoIP protocol identifier used for valid packet distinguishing by the function fD. Header length that contains the total length of AoIP header,
2. *Token* length that contains the length of a user token *t*,
3. *Checksum* length, specifying size of the checksum *c* element,
4. *Unique packet number* (r),
5. *User token* (t),
6. *Checksum* (c).

As presented in the illustration (Fig. 8) the AoIP segment containing elements 3–7 is encrypted. The encryption details are described as preliminary assumptions for implementation later in this article.

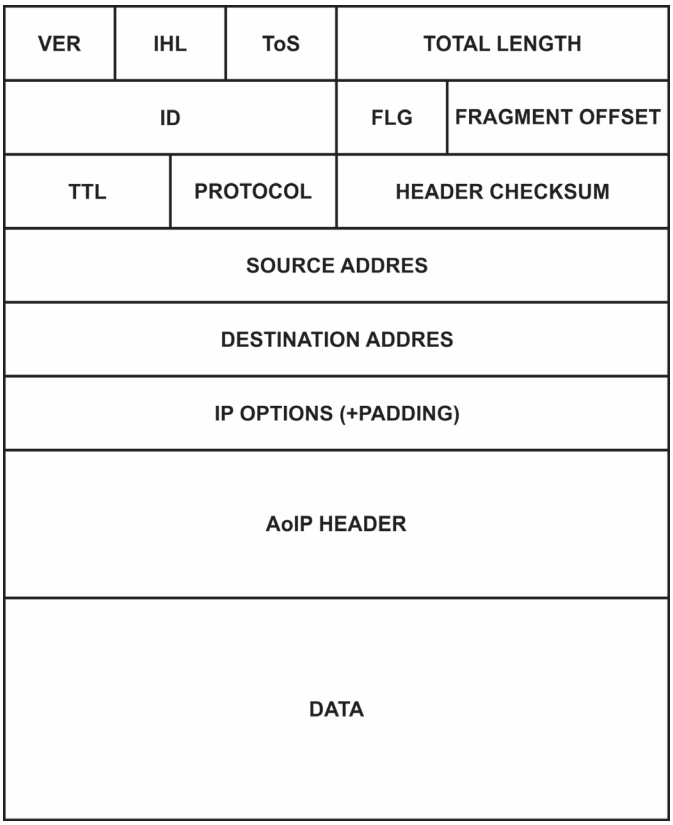

Fig. 8. AoIP header structure

3.2.2. Operation diagram. The communication using AoIP protocol may be described as follows:

Sender

1. The identity data (a smart card, fingerprints, creden-tials, etc.) is provided by a user,
2. User attempts to apply service at receivers,
3. The AoIP transmission service processes each IP packet to an authenticated packet:
   a) IP packet data checksum c is calculated,
   b) AoIP header is created,
   c) the AoIP header segment is encrypted,
   d) the IP packet is extended with AoIP header and the *total length* field is altered; while the IP packet is fragmented when necessary.
4. Transmission service dispatches the packet through public network.

Public network

1. The packet is transmitted to the destination using existing IP infrastructure. It is exposed to interception, modi-fication and multiplication.
2. The encryption prevents the token from being revealed and the checksum *c* ensures the packet integrity.

Receive

1. A border device separates authenticated and not authenticated packets on the basis on AoIP ID.
2. Each authenticated packet is validated as follows:
   a) AoIP header length is read,
   b) an encrypted AoIP header segment is decrypted,
   c) the uniquity of r (packet unique number) is checked,
   d) a user token t is validated,
   e) IP packet data checksum is calculated and compared with the checksum c from AoIP header,
   f) finally, the entire AoIP header is removed from the packet, and the orginal *Total length* field value is restored.
3. The IP packet is transmitted to the destination server.

3.2.3. Preliminary assumptions for implementation. The presented concept is currently being implemented. This article presents its basic assumptions regarding the authenticated packet structure and operation diagram. This paragraph describes assumptions that are taken into consideration at the early stage of its implementation, however these are not final and will be reviewed in the future.

As it has been mentioned above, a user token t has not been tightly related to any particular user identification method. From the point of view of implementation, it is a form of binary data, and its length may vary for different generation and serialization methods.

The unique number r for each subsequent message M_i and each packet v_{Aj} is formed as follows:

$$r_{i,j} = r_0 + \sum_i n_i + j,$$

where n_i stands for a number of v_A packets in message M_i and r_0 is a periodically and randomly selected number based on time and/or senders address (i.e. IP number). The algorithm consists in selecting a random number and incrementing it by 1 for each authenticated packet sent. It seems reasonable to consider the MD5 [28] or SHA-3 [29] as a checksum generation algorithms. The AoIP header will be encrypted using a public key of the receiver with symmetric encryption algorithm (RSA [30], DSA [1], ECC [31]). Implementation plans are discussed in the next section of the paper. The plans include selection of valid algorithms and methods for the problems described above.

3.3. Summary. In this part of the paper a general concept of packet transmission authentication was presented along with its application to IP protocol (AoIP). The idea meets basic

assumptions stated at the beginning of the research works. A set of assumptions has also been collected for further implementation.

The main advantage of AoIP is the capability of background processing on user's demand without high performance requirements and preventing transmission from embezzlement. The proposed algorithm does not exclude possibility to use additional security mechanisms, like IPSec or other secure transmission methods, especially at application layer (HTTPs, TLS).

What is more, the concept introduces user's priorities and eliminates their anonymity. The possibility of simultaneous processing of AoIP and non-authenticated packets enables the user to decide whether to take advantage of better service at the cost of rejecting the anonymity.

The concept does not present any compatibility problems with the existing services and transmission methods, as it operates at the network layer of IP communication. There is no need to implement adjusted software which is required to deploy other methods (i.e. Kerber-os).

Moreover, the implementation of the firewall rule enables simple packet filtering without any additional processing and computing.

4. Discussion

As it has already been mentioned, any authentication method that is intended to enhance the security level increases the number of components vulnerable to overload [8]. The proposed method introduces a new layer in the communication model. If the additional layer is processed at the software level, it requires additional CPU load and utilizes more memory, which has to be considered as another potential weak point. The answer to this problem may be the application of hardware components, that would handle the most demanding tasks (such as encryption or checksum calculation). This will also result in better transmission throughput that may be slightly limited in case of the software approach.

Various methods of authentication and authorization have been successfully implemented in network devices, especially in routers and firewalls. These kinds of devices are designed to prevent transmission into internal network, even if the DoS attack occurs. It is supposed that AoIP implementation in such devices should not limit their throughput.

The fact that the IP packet includes AoIP header also creates the problem of enlarging the actual transmitted data size, which may lead to limiting the transmission throughput. This issue may be considered in two different ways. Firstly, the network transmission throughput is constantly increasing and it has already reached a point, where a relatively small surplus of transmitted data should not deteriorate online services utilization. Secondly, the AoIP header size depends on the imple-mentation details. The header size can be adjusted to obtain satisfactory level of security and transmission throughput.

The features of the proposed method are compared to NTLM, IPSec and WireGuards solutions mentioned herein. The results are presented in Table 1. But the main difference is that proposed method is the lightest one. So, the best advantage of this method is that it could be implemented in light IoT (Internet of Things) devices. The authors of WireGuard describe it as light solution, as it has only 4000 lines of code, but this number does not include the crypto-primitives which it uses. So it will be hard to implement it in the solutions which do not use the whole system implementation as Linux.

Table 1
Method comparision

Features comparision
Kerberos: • complexity: high, • Sensitive on DoS attack: yes, • possible throuput: – • connetionsless: no
NTLM: • complexity: high, • Sensitive on DoS attack: yes, • possible throuput: – • connetionsless: no
IPSec: • complexity: high, • Sensitive on DoS attack: yes, • possible throuput: depends on computational power • connetionsless: establish a network interface
WireGuard: • complexity: average, • Sensitive on DoS attack: yes, • possible throuput: depends on computational power • connetionsless: establish a network interface on UDP
AoIP: • complexity: low, • Sensitive on DoS attack: no, • possible throuput: high, should not have impact on network • connetionsless: do not establish a network interface

Testing possible network throughput by using different solutions provides results which are difficult to compare. This is due to the fact that IPSec and WireGuard are designed to protect the whole network, while the proposed AoIP is intended for network protection against DoS attacks, and it operates on client site and the router of protected network, rather than at the router-to-router connection.

5. Further work

Further development of the IP packet authentication concept is planned. Currently, the sender and receiver software for AoIP communication is under development. The implementation is based on the following components:

- service for users taking advantage of AoIP,
- service for servers that will be able to receive au-thenticated IP packets.

Both services are implemented on Microsoft Windows platform for research purposes.

The next stage is the development of a cluster of servers on the receiver side which would enable traffic balancing and evaluate the scalability. For the traffic balancing, Vyatta router has initially been chosen.

The third stage is the evaluation of different checksum calculation algorithms, user token generation and AoIP header encryption. The evaluation includes performance, header size and hardware component application analysis. This part of the research also includes risk analysis for each algorithm involved. The last stage will be the analysis of the possibility to replace current authorization methods at the application level for computer system services and applications currently under development. One of the main problems is the security of the proposed method. The main vector of the attack which has to be blocked is the attack on sequence numbers r. The attack could result in the increase of the computational power required for processing the packet transmission, because the AoIP operates as software. The solution aimed at avoiding such attack is an encryption of IP header, and, as it was mentioned above, it could be achieved using a public key of the receiver with symmetric encryption algorithm (RSA [4], DSA [28], ECC [6]).

Such encryption will use less computational power than the encryption of entire IP packets, but it required implementation of encryption algorithms. In such cases it will be more difficult to implement the proposed method to IoT solutions. The other important case is the length and recommended lifetime of the keys. It is well known that if the key is longer and key exchange is frequent, the security of the solution is better. However, the key length and exchanging process determine the required computational power and network throughput. Thus the authors claim that these parameters will be determined depending on the system to which the method is to be implemented. In the case of small solutions, such as small IoT devices, the keys will be shorter than in huge systems such as the Cloud System, in which the computational power is almost unlimited. The implementation shall provide a flexible configuration scheme as per the network requirements.

There is obviously a plan to check the entire security of the proposed method. The authors expect that this analysis shall decide whether the proposed solutions have achieved the expected security level or have still to be improved. It is unclear whether the use of sequence numbers r against replay attacks requires a sliding window scheme.

6. Conclusion

This paper presents the concept of IP based authentication of communication transmission. One of the essential features is the capability to apply the idea in the existing network based on IPv4, which provides data transport from the sender to the receiver.

The implementation of this method should substantially limit the risk of successful DoS attack for publicly available systems.

Moreover, the AoIP method is a good supplement to existing protocols that provide secure connection and stable online operation. With the AoIP, the problem of service blocking by groups of hackers will be significantly reduced. The future implementation shall verify the assumptions of this paper.

The above qualities of the AoIP concept suggest that the method is prospective for future network communication.

Finally, it should be pointed out that the authors will highly appreciate any opinions and evaluations concerning this concept.

References

[1] C.E. Shannon, “A mathematical theory of communication”, *The BELL System Technical Journal* 27, 379–423 and 623–656 (1948).

[2] IBM Knowledge Center, (last modified 2012) [Online]. Available: http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp? topic=%2Fewlminfo%2Feicaawkldbalancing.htm [Accessed: 22-Feb-2020].

[3] B. Dowling and K. Paterson, “A cryptographic analysis of the wireguard protocol”, in *ACNS*, 2018.

[4] RSA Laboratories. PKCS 1 v2.1: RSA Cryptography Standard June 2002, (last modified 2012) [Online]. Available: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2- 1.pdf [Accessed: 22-Feb-2020].

[5] Open source router and firewall platform, (last modified 2019) [Online]. Available: https://vyos.io [Accessed: 22-Feb-2020].

[6] “Standards for efficient cryptography.” Technical report, SEC 1: Elliptic Curve Cryptography, 2012.

[7] D. Mazur, A. Paszkiewicz, M. Bolanowski, G. Budzik, and M. Oleksy, “Analysis of possible sdn use in the rapid prototyping pro-cess as part of the industry 4.0”, *Bull. Pol. Ac.: Tech*., 67(1), 21–30 (2019).

[8] Rewolucja w bezpiecznych połączeniach VPN z WireGuard, (last modified 2019) [Online]. Available: https://www.hostersi.pl/rewolucja-wbezpiecznychpolaczeniach-vpn-z-wireguard/ [Accessed: 22-Feb-2020].

[9] “Request for comments 791, protocol specification.” Technical report, Information Sciences Intitute, September 1981.

[10] SHA-3 project, (last modified 2019) [Online]. Available: https://csrc.nist.gov/projects/hash-functions/sha-3-project [Accessed: 22-Feb-2020].

[11] Kerberos FAQ, v2.0, (last modified 2000) [Online]. Available: http://www.faqs.org/faqs/kerberos-faq/general/ [Accessed: 22-Feb-2020].

[12] R. Rivest, “Request for comments: 1321, The MD5 message digest Algorithm”, Network Working Group, April 1992.

[13] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. “The kerberos network authentication service (v5). Request for Comments: 4120”, Network Working Group, 2005.

[14] C. L. Schuba, M. G. Huhn, E. H. Spafford, and A. Sundaram. “Analysis of a denial of service attack on tcp.” Computer Science Technical Reports, 1327, 1996.

[15] R.K.C. Chang, “Defending against flooding-based distributed denial-of-service attacks: a tutorial”, *IEEE Commun. Mag*. 40, 42–51 (2002).

[16] D. Moore, G.M. Voelker, and S. Savage. “Inferring internet denial-of-service activity”, *ACM Trans. Comput. Sys*. 24, 115–139 (2006).

[17] P. Pietkiewicz, K. Nalepa, W. Miąskowski, and M. Wilamowska-Korsak, "A system for monitoring and controlling a thermal energy store and an energy capture system", *Bull. Pol. Ac.: Tech*., 66(6), 941–946 (2018).

[18] VYATTA, (last modified 2008) [Online]. Available: http://www.vyatta.com [Accessed: 22-Feb-2020].

[19] M. Chiang and A.R. Calderbank. "Layering as optimization decomposition: A mathematical theory of network architectures", Proceedings of the IEEE, 95, 255–312 (2007).

[20] J.K. Millen, "A resource allocation model for denial of service", *IEEE Computer Society Symposium*, 137–147 (1992).

[21] S. Kent and K. Seo, "Request for comments: 4301, security architecture for the internet protocol." NetworkWorking Group, December 2005.

[22] S. Kent, "Request for comments: 4302, ip authentication header." Network Working Group, December 2005.

[23] GNU shishi, (last modified 2002) [Online]. Available: http://www.gnu.org/software/shishi/ [Accessed: 22-Feb-2020].

[24] M.A. Sirbu and J.C.I. Chuang, "Distributed authentication in kerberos using public key cryptography", *Network and Distributed System Security*, 134–141 (1997).

[25] B.C. Neuman and T. Ts'o, "Kerberos: an authentication service for computer networks", *IEEE Commun. Mag*., 32, 33–38 (1994).

[26] Heimdal kerberos and security software, (last modified 2008) [Online]. Available: http://www.h5l.org/ [Accessed: 22-Feb-2020].

[27] C. Meadows, "A formal framework and evaluation method for network denial of service", *IEEE Computer Security Foundations Workshop*, 4–13 (1999).

[28] "Digital signature standards (dss)." *Technical Report* vol. 74, pp. 27287–27288, National Instituite of Standards and Technology.

[29] Microsoft NTLM, (last modified 2012) [Online]. Available: http://msdn.microsoft.com/enus/ library/ windows/desktop/ aa378749(v=vs.85).aspx [Accessed: 22-Feb-2020].

[30] J. Donenfeld, "Wireguard: Next generation kernel network tunnel", in 24th Annual Network and Distributed System Security Symposium, (2017).

[31] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for ip traceback un-der denial of service attack", Computer Science Technical Reports, (2007).