UDC 004.9/.04

Intrusion detecting systems and blockchain technology

Eduard Sikolenko[1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Beresteyskyi ave., 37, Kyiv, 03056 Ukraine*

Abstract

In this article, the information about intrusion detection systems and intrusion prevention systems was analyzed. General information, differences, main advantages and disadvantages of intrusion detection and prevention systems were described. The blockchain technology was analyzed as well. The main information on the blockchain technology was shown: the history of creation, sphere of application, working principle, potential threats and specifics of consensus mechanism. Based on the information given, it is planned to apply the blockchain technology in intrusion detection systems to increase the level of security.

Keywords: Intrusion Detection System, IDS, IPS, Blockchain, Consensus Mechanism

Introduction

According to the European Union Agency for Network and Information Security statistics, the number of cyber threats in 2024 increased by two times, comparing to 2023. The total number of cyber incidents was 11 079 for the period from July 2023 to June 2024 [1]. The fact that the number of threats is increasing requires the development of new approaches for protection of the information systems.

One of the latest approaches is the use of blockchain technology. Due to its consistency, the mentioned technology is able to provide a high level of protection and increase the efficiency of cyberattack detection, as well as provide a rapid response to security incidents.

1. IDS and IPS systems

The intrusion detecting systems (IDS) and instituting prevention systems (IPS) were designed to protect network and information systems from threats. IDS and IPS provide higher level of protection than antiviruses, spam-filters and firewall, however the last-mentioned systems should be present as a part of cyber security: it is better to combine all these methods to achieve the highest level of protection [2].

IPS and IDS systems do not require in-depth knowledge to set up successfully, are easy to maintain, and can provide high accuracy in network monitoring [2]. These systems provide the ability to detect signatures, anomalies and can monitor user activity to detect unusual behavior.

The most well-known IDS and IPS systems are:

- Snort
- Suricata
- McAfee Network Security Platform
- Zeek
- OSSEC
- Wazuh
- TippingPoint

1.1. IDS and IPS working principle

To start with, there are two main modes of operation of intrusion systems [3]:

- Finding correlation with signatures
- Detect anomalies in user activity

Signature is a predefined pattern that is used to identify specific malicious activity. Finding correlation with signatures is crucial. With the help of signatures IDS and IPS may detect the attack. However, this operation mode requires up-to-date signature base. Multiple sources of signature data are obligatory condition for high-level security.

The second mode is related to detecting anomalies in user and process activity. Thus, an attempt to perform a suspicious action, an attempt to perform an action prohibited by rights, an unexpected attempt to scan the network, making requests at untypical time or sending requests too frequently, authorization errors, etc. can be considered as an attack.

To detect intrusions, it is also possible to configure a client's geographic location check.

As a result, it is important not only to look for matches in signatures: but also to understand the attack scheme and try to predict the next steps of the attacker. The IDS and IPS systems shall automatically collect all the necessary data and find connections between suspicious events.

1.2. Difference between IDS and IPS systems

The main difference between IDS and IPS is that IDS monitors traffic and compares it with existing signatures, but does not repel attacks on systems, because it processes a copy of the traffic, allowing the main traffic to enter the network.

This means that IDS is designed to detect intrusions and inform about possible intrusions. On the other hand, IPS checks traffic for compliance with existing signatures, but if risks are detected, it not only notifies the system administrator but also automatically blocks dangerous traffic.

Talking about the positioning of IDS and IPS – IPS stands across the network traffic, however IDS stands near the network [4]. This aspect is illustrated in Figure 1.

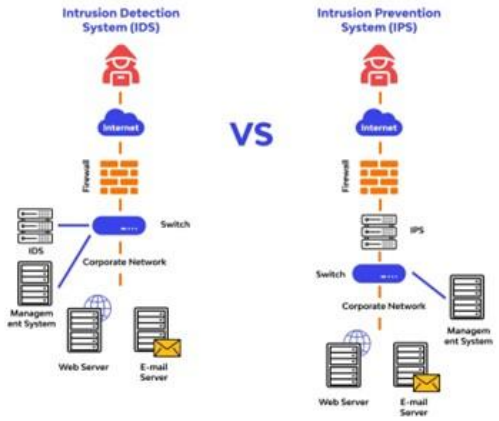

Figure 1: The difference in the positioning of IDS and IPS systems

According to the information given above, the main advantage of IDS is that IDS does not affect the traffic flow and the speed of packets through the network. One more advantage of IDS is that this type of protecting system does not create additional workload on the network hardware.

On the other hand, IDS can only detect potential threats. That meant that the system administrator should always be ready to analyze recognized anomalies and start to repel an attack.

1.3. The ideal IDS system

Based on the information about the working principle, several requirements for the ideal IDS and IPS systems are set [5]:

- Finding correlation of signature data from multiple sources
- The possibility of profiling
- Availability of behavioral analytics and the ability to detect anomalies
- Evaluation of user and system activity
- Ability to integrate machine learning
- Mitigate false alarms

2. Blockchain

To start with, blockchain was invented in 2009. The main run force of this invention was the development of crypto coins, namely bitcoin. Humanity has responded positively to the development of blockchain technology, which has contributed to its further spread in the economy [6].

Currently, blockchain technology is used not only in the banking sector, but also in public administration, law, creation of digital identity cards, etc.

2.1. General information about blockchain

Blockchain is a decentralized database that stores an ordered chain of data. This chain could add new blocks to it. Each block contains information on the time stamp of creation, the hash of the previous block and transaction data. The information contained in the chain is protected from forgery and distortion.

The main properties of blockchain are [6]:

- **Transparency**: the chain has the entire transaction history from the moment the chain was created
- **Stability**: distortion and/or deletion of information in block is not possible unless the parties of the transaction agree
- **Independence**: the chain is decentralized. That means that each network participant stores all the information about the chain on his/her device

These properties are achieved through the consensus mechanism. It is responsible for confirming transactions and validating them. The protection of this mechanism is one of the most important issues arising from the presence of decentralization in blockchain technology.

2.2. Blockchain structure

As was mentioned earlier, in blockchain technology, each block contains a hash of the previous block. This makes it possible to link the blocks together and makes it impossible to change any block or add a new block between two other blocks without acceptation of all the parties of the blockchain network [7]. The structure of the blockchain is shown in Figure 2.

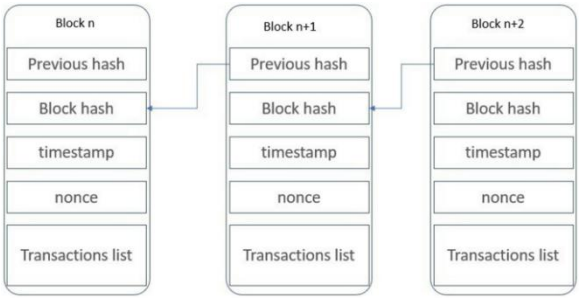

Figure 2: The structure of blockchain

As blockchain is a decentralized database, the structure of its network may be represented as shown in Figure 3.

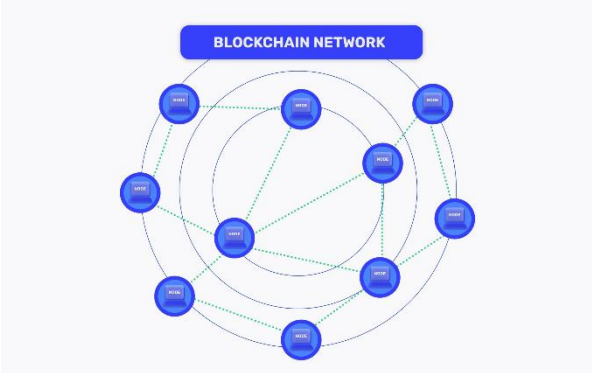

Figure 3: The structure of the blockchain network

Each member of this network is named as node. In Figure 3, it is shown that the blockchain network does not have a database server, and all the information about the blockchain network is stored at each node.

It is important to note that there are two types of users in blockchain [8]:

- **Full node**: this type of node stores all the information about transactions
- **Light node**: this type of node stores only obligatory information about transactions

Full node stores all the information about blockchain structure and its size may be counted in dozens of terabytes. Light node stores only obligatory information, and its size may be evaluated as one-two terabyte. Light node may ask Full node to obtain the information about specific transaction.

2.3. Consensus mechanism

Consensus mechanism is a self-regulating protocol stack that synchronizes the network to coordinate it. Consensus in decentralized systems is necessary to ensure that the system is fair to all participants. This mechanism is used when creating new blocks, so the security of data and users in the blockchain network directly depends on the protection of this mechanism.

There are a lot of different protocols, however, there are two main protocols [7]:

- Proof of Work (PoW)
- Proof of Stake (PoS)

The information about these consensus mechanisms will be provided below.

2.3.1. Proof of Work consensus mechanism

In Proof of Work consensus mechanism, the nodes shall perform computational work in order to create a new block and add it to the chain. The node that wants to add a new block (this node is called miner) needs to find the right hash for the new block, however this hash shall meet some specific conditions of blockchain network (for example, to start with zero, etc). Hash of the created block may be changed with the help of nonce – random number that need to be changed in order to satisfy specific conditions [9].

When the miner finds the right nonce, he notifies all the members of the blockchain network, so everyone may check whether the block may be created. If all the requirements are fulfilled, the new block will be added to the chain.

The main advantage of PoW is a high level of security; however, it also has some disadvantages:

- High energy consumption to create new block, as a lot of computational work is performed
- Low scalability, as the creation of new blocks is time-consuming

It is important to mention that there are some possible types of attacks at PoW [7]:

- **51% Attack**: the miner that has more than 50% of computing power may change transaction history or perform double spending attack
- **Selfish mining**: the miner that has enough computing power may try to create a new chain of blocks. This may be possible if the attacker does not broadcast the block as soon as it is found, and tries to create a new chain, that is longer than the public chain. This also may lead to a double spending attack
- **Double spending attack**: the miner that has enough computing power may try to perform two transactions at the same time, and, therefore, two following chains may be created. This may lead to double spending of blockchain coins by honest nodes

The most popular blockchain networks that use PoW are Bitcoin, Litecoin, Vertcoin.

2.3.2. Proof of Stake consensus mechanism

Proof of Stake consensus mechanism is an alternative to PoW. PoS allows nodes to create new blocks without a large amount of computing power. Thus, to create a block in PoS, nodes should lock up some number of coins as a stake. The node that will create a block is elected randomly, however, the more coins the node stake, the more chance the node has to be elected.

When the node is chosen to create a block, he shall validate the transaction and share the new block to the blockchain network. Other parties confirm the validity of the new block and agree to add it to the chain.

The advantages of the PoS are the following:

- Low energy consumption to create and validate a new block
- High scalability, as miner does not perform a lot of calculations to create a new block
- Special hardware is not needed
- Availability of penalties: nodes may lose all their stake, if they act maliciously

The disadvantages of PoS are listed below:

- Nodes with larger stakes have higher probability to be elected as block creators. This may lead to centralization of coins in one node
- Security weakness of the new blockchain network, as nodes may not have enough stake to ensure needed level of security

PoS may also be a subject to some types of attacks, namely [7]:

- **51% Attack**: the principle is the same as in PoW, however, the main resource of such attack in PoS is stake, not computing power
- **Nothing-at-Stake Attack**: as creation of blocks is quick and easy in the sense of computing power, the attacker may create several chains, making the network lose the right chain
- **Stake Grinding**: the attacker may try to manipulate with random mechanism (for example by finding some correlations among the chosen nodes) and get privilege over the other miners
- **Censorship attacks**: the nodes that have enough stake may collude and deny valid transactions, for example, to give privilege to some specific node

There are also different variants of PoS consensus protocol, however, the main principles of their work are the same: light computing processes and usage of a stake. Some of them are: Delegated Proof of Stake, Leased Proof of Stake, Secure Proof of Stake, Nominated Proof of Stake, Effective Proof of Stake, Liquid Proof of Stake.

The most popular blockchain networks that use PoS-based consensus algorithm are Ethereum, Cardano, Binance Smart Chain, Algorand.

2.4. Application of blockchain in IDS

Certainly, blockchain technology has a lot of benefits, therefore, this technology may be applied in IDS systems. The usage of blockchain may increase the effectivity of IDS and IPS systems. This may be achieved by creating a blockchain-based trusted IP addresses list, list of trusted informational resources, trusted email addresses, etc. Furthermore, with blockchain, it is possible to create new methods of organization of monitoring systems and incident analysis. Last but not least, the new systems for broadcasting of the information about new threats may be created with the help of blockchain [10].

However, it is probably better to create such blockchain networks not to store the information about trusted resources, but to store the information about untrusted resources: emails that send spams, IP addresses that scan websites, and so on. This is explained by the fact, that it is easier to store the information about threats, as there are much more safe data, than dangerous.

Conclusions

The main purposes of IDS and IPS were described, as well as its working principle. In addition, blockchain technology was observed, including the indication of its benefits and drawbacks. Kudin A.M. proposed some applications of the usage of blockchain technology in the field of cybersecurity.

In further researches it is planned to expand the list of possible applications of blockchain technology to increase the effectivity of IDS systems. The next step is to create an application that will use blockchain in IDS.

References

[1] ENISA, *ENISA THREAT LANDSCAPE 2024*. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

[2] T.I. Korobeinokiva and O.O. Tsar, ”Analysis of modern open intrusion detection and prevention systems”, (in Ukranian), *Grail of Science*, vol. 27, pp. 317-325, 2023. doi: 10.36074/grail-of-science.12.05.2023.050

[3] B. Lokesak, ”A Comparison Between Signature Based and Anomaly Based Intrusion Detection Systems”, Bloomington, IN, 2008.

[4] IPS. vs. IDS vs. Firewall: What Are the Differences? [Online] Available: https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips

[5] A.S. Yanko and O.I. Makarenko, ”Concept of a network intrusion detection and prevention system”, (in Ukranian), *Control, navigation and communication systems*, vol. 2, pp. 59-67, 2022. doi: 10.26906/SUNZ.2022.2.059

[6] Y. Grudzevych, O. Kleban, U. Buluk and M. Rondiak, ” Emergence and prospects for the development of blockchain technologies in Ukraine”, (in Ukranian), *Economic Journal of Volyn National University*, vol. 3 no. 23, pp. 162-167, 2020. doi: 10.29038/2411-4014-2020-03-162-167

[7] E. V. Shevchuk and V. M. Fedorchenko, ”Analysis of the main vulnerabilities and ways to protect the consensus mechanism in decentralised blockchain systems *Control, navigation and communication system* vol. 3, pp. 170-174, 2024. doi: 10.26906/SUNZ.2024.3.170

[8] Cryptopedia, ”Types of Nodes: Light Nodes, Full Nodes, and Masternodes”, 2021. [Online]. Available: https://www.gemini.com/cryptopedia/masternode-dash-bitcoin-node

[9] The Investopedia Team, ”Nonce: What It Means and How It’s Used in Blockchain”, 2024. [Online]. Available: https://www.investopedia.com/terms/n/nonce.asp

[10] A. M. Kudin, ”Blockchain in cybersecurity: theory and practical application”, (in Ukranian), *Visn. Nac. Akad. Nauk Ukr.* 2024. (7): 31—36. https://doi.org/10.15407/visn2024.07.031