International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)
ISSN: 2305-0543 (Online), ISSN: 2411-6173 (Print)
Vol. 12 (46), Oct. 2022, pp. 5293-5296

Modern Networks' Security: Problems and Challenges

Somayyeh Iman Alizadeh
Islamic Azad University, Shahriyar Branch,
Shahriyar, Iran
imanalizadehsomayeh@yahoo.com

***Abstract*— Online social networks (OSNs) are intertwined as a necessary tool in the modern world in conveying messages to the community with security issues. New and modern mass media play a significant role in producing security because part of the insecurity and lack of secure feeling is caused by its quick redistribution. It means that new tools are one of the main factors of social awareness and obtaining information about the events happening in the surrounding environment. In the modern era, considering that life is surrounded by new media, including Telegram and...., the level of anxiety and insecurity of people has also increased and people are inevitably placed in the media's publishing structure. According to studies, social network users easily expose their confidential details and personal information to others. Abuse of this information in the virtual and real world can cause harm. But keep in mind that there are many modern software solutions and methods that help users against threats.**

Keywords*— social networks, security, media, Internet, Network security, Data security

I. INTRODUCTION

The Internet is a huge information network and an extensive information bank that will be accessible to every single person in the near future. Communication experts consider the use of this network to be a must in current era[1]. Consisting of thousands of smaller networks, regardless of geographical boundaries, it has connected the whole world together. According to the latest statistics, more than sixty million computers from all over the world are connected to each other in this vast network, which provides infinite information in all fields and they have shared all kinds of things. It is said that nearly one billion pages of information on various topics have been placed on this network by real and legal persons [2]. This information is exchanged rapidly between users in data highways and there is no restriction or control on entering or receiving data. Supporting the free flow of information, the increasing expansion of information technology and creating a platform for connecting to information networks is the governments' motto. Meanwhile, the extent and variety of unhealthy information on the Internet has caused concern among different countries. The publication of obscene images, the creation of websites with pornographic themes and child abuse sites and all kinds of trafficking in advanced industrial countries, especially in the origin of this global network, which is the United States, have greatly worried social experts, forcing the governing committee to adopt laws to control this network in the United States. Warnings, fines, and arrests for those who set up destructive and corrupting sites are the measures that different countries of the world have taken to deal with the destructive effects of the Internet[3].

The fear of the destruction of moral and social foundations, caused by the invasion of unhealthy and destructive information through the Internet, is a logical reaction, because every society has its own information frameworks, and it is natural that any type of information that breaks these limits and boundaries can endanger the health and safety of the society. Despite the positive aspects of global networks, the misuse of these computer networks by criminals has put the national security in danger in different countries. Hence, the use of filters and various firewalls are increasing to prevent the penetration of malicious and harmful data and to select healthy information in these networks. Fortunately, despite the existence of commotions that Internet as uncontrollable, the technology required to control this network and select healthy information is expanding and evolving [4].

II. NETWORK SECURITY CONCEPT

Network security includes regulations and policies decided by network management, which are compiled and applied in order to prevent and monitor unauthorized access, abuse, modification, or restriction of computer networks and available resources in the network. Users choose or they are assigned an ID and password or other authenticating information that allows them to access information and programs within their domain. Network security covers all types of computer networks, both public and private, that are used in everyday business: transactions and communications between businesses, government agencies, and individuals. Networks can be private, such as within a company. Network security plays an important role in organizations, businesses, and other types of institutions. The most common and easiest way to protect a network resource is by assigning it a unique name and a corresponding password [5].

The terms "network security" and "information security" are often used interchangeably. Lack of knowledge in many users and employees of organizations helps intruders to easily enter a computer network and obtain confidential information or engage in destructive activities. The more the Internet and the information on it grow, the more the importance of network security. Network security is generally used to provide the ability to protect the boundaries of an

Article History:
Received Date: May. 14, 2022, Accepted Date: Jul. 11, 2022, Available Online: Oct. 01, 2022

organization against intruders (such as hackers). To ensure security on a network, one of the most critical and dangerous steps is to provide secure access and control network equipment such as routers, switches or firewalls. However, information security is clearly focused on protecting information resources against virus attacks or simple mistakes by people within the organization, and for this purpose it uses data loss prevention techniques. One of these techniques is the division of large networks by internal boundaries[5]. Network security starts with user authentication, usually with a username and a password. Since this requires only one thing besides the username (i.e. password), it is sometimes called "single factor authentication".

With "two-factor authentication" something you have is also used (for example, a security token or hardware lock, an ATM card or your mobile phone), or with "three-factor authentication" something that proves your identification is also used (such as a fingerprint). After authentication, the firewall implements access policies, such as what services are allowed to be available to network users. However, to prevent unauthorized access, these components may fail to check for potentially harmful components, such as computer worms or Trojans transmitted over the network.

Anti-virus software or intrusion prevention systems (IPS) are of great help in identifying and inhibiting the operation of such malicious software. An anomaly-based intrusion detection system may also monitor the network and its traffic in terms of unwanted and suspicious content or behavior or other anomalies to protect resources, for example, denial of service or access to employee files at unusual times. Unique events that occur in the network may be recorded to be reviewed and analyzed at a higher level in the future [6].

- **Security management**

Security management for networks is different for different types of situations. A small house or an office only needs basic security; while large businesses need high-level protection and advanced software and hardware to prevent malicious attacks such as hacking and sending anonymous emails.

- **Data security risk evaluation**

Risk evaluation is the most important part of the data security risk management process. As shown in the figure, this process includes creating context, risk evaluation, risk exposure, risk acceptance, risk monitoring and risk investigation. The data security risk management process can be repeated for risk evaluation or risk elimination activities [7].

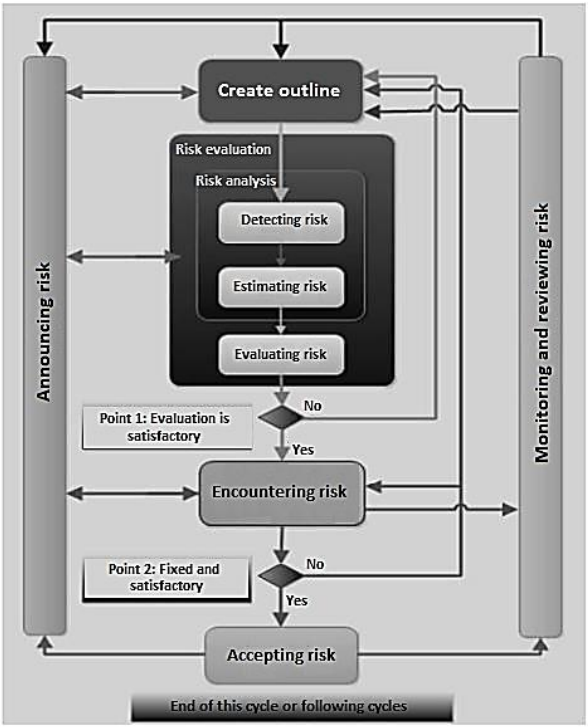
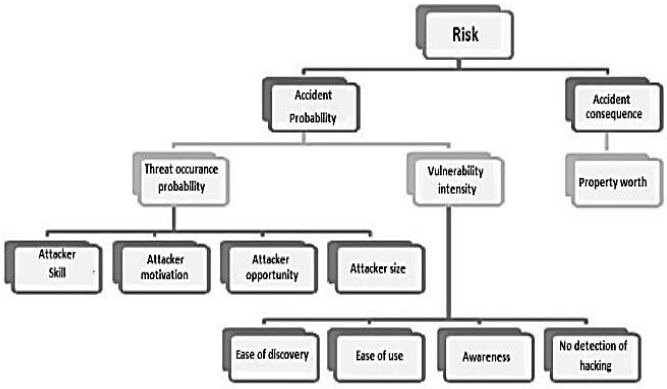


Figure 1: Data security risk management procedure

III. The Proposed Model to Evaluate Data Security Risk

Risk is a function of "probability of accident" and "consequence of accident". "Threat probability" and "vulnerability level" are components of accident probability. The main issue in risk evaluation is determining the indicators that affect the probability of the threat and the level of vulnerability. The proposed model and related indicators are shown below. The possibility of threat: Four indicators for the possibility of threat are:

- Attacker skill
- Attacker motivation
- Attacker opportunity
- Attacker size



The proposed model for evaluating risk

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

The scales related to the attacker skill criterion is shown in Table below:

Skill evaluating scale	Description
Very little	Threatening group don't have technical skills
little	Threatening group has little technical skills
Average	Threatening group are advanced users
much	Threatening group have programming and network technical skills
Very much	Threatening group have security hacking skills

The scales related to the attacker motivation criterion is shown in Table below:

Skill evaluating scale	Description
Very little	Threatening group have very little motivation to threaten
little	Threatening group have little motivation to threaten
Average	Threatening group have some motivation to threaten
much	Threatening group have much motivation to threaten
Very much	Threatening group have very much motivation to threaten

The scales related to the attacker opportunity criterion is shown in Table below:

Skill evaluating scale	Description
Very little	Threatening group do not access to special data
little	Threatening group have access to limited and special resources
Average	Threatening group have access to average amount of resources
much	Threatening group have access to special resources
Very much	Threatening group have complete access to very special resources.

The scales related to the attacker size criterion is shown in Table below:

Skill evaluating scale	Description
Very little	Threatening group is limited to developers
Little	Threatening group includes system managers
Average	Threatening group includes internet users
Much	Threatening group are all authorized users or partners
Very much	Threatening group includes all internet users

In this article, it should be considered that one of the threats of social networks are modern threats. These threats usually target people's information as well as the personal information of the target's friends. For example, an attacker trying to access a user's school name on Facebook (the account is only visible to the person's Facebook friends) can create a fake account with the appropriate details and send a friend request to the target user. If the user accepts the friend request, the details of the information will be visible to the attacker. In addition, the attacker will have access to the data of the user's Facebook friends and implement an inference attack.
Security and media in the modern era are two interrelated categories that human society is involved in. Today's world is the world of mass media and its widespread presence in people's lives, which has affected social security[8]. To prevent social threats, modern security has provided solutions:

- Authentication
- Security and privacy settings
- Internal protection mechanisms
- Users report
- No location release and...

In research titled "Application of virtualization in improving the security and reliability of SCADA software and power grid automation", Giveei and Kerami [9] reached these results: in this article, first, a step-by-step method for applying virtualization technology in the installation and operation of SCADA and post automation systems is introduced in order to achieve the capabilities of this technology. This method can be used by all experts and engineers in the field of dispatching and power network automation. For a better understanding, it is also described with a case study of SCADA software and ABB MicroSCADA pro post automation. According to the results obtained, in addition to access to modern technologies and

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

the inherent and significant features of virtualization, with the help of this technology, improvements in time and cost is also achieved.

Ghafarpour, Poormousa and Ranjbar [10] in research titled "Presenting a criterion for evaluating power network security using fuzzy logic theory" reached these results: In this article, to evaluate the security of the power system by considering the uncertainty in power injection to network, a hybrid method based on probability theory and possibility theory was presented. Based on this, an intensity function is determined for each of these parameters. The obtained criterion is not related to the risk of the entire network, but it is calculated separately for each bus and with one network line. According to this, power system planners can use these criteria for future planning of the system as well as network security evaluation.

Asgarian Abianeh et al. [11], in research titled "Planning the development of the transmission network under the conditions of the electricity market, taking into account the cost of establishing security", reached these results: a new strategy for designing the development of transmission lines was discussed and reviewed in this article that in this method, in addition to other effective factors in the design of development under the conditions of the electricity market, the minimum cost of establishing security is also included. This cost is calculated based on minimizing the cost of disconnecting the load due to the occurrence of critical conditions. This cost is different for various development designs. As a result, by taking it into account during the design, it is possible to direct the design towards a more stable and economical network. Planning the development of the transmission network for wide networks using the mentioned method requires the use of a sequential algorithm. By using this algorithm, one of the best answers in the solution space with a probability of almost 100% will be obtained.

IV. CONCLUSION

So far, many solutions have been proposed to deal with the problem of information security risk evaluation. One of these solutions is risk evaluation using smart methods. In this article, the method of artificial neural networks is used for risk evaluation, with this new method, more realistic criteria were defined for risk effective factors, which makes the results more accurate and closer to reality. Surveys show that consensus exist among international information security experts about these criteria. Investigations showed that the results of neural networks have higher accuracy and quality compared to other methods.

REFERENCES

[1] Tounsi W, Rais HJC (2018) A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur 72:212–233.

[2] Mokhtar B, Azab MJAEJ (2015) Survey on security issues in vehicular ad hoc networks. Alex Eng J 54(4):1115–1126.

[3] Ganji, Alireza (2022), network security, challenges and solutions

[4] Asgharzadeh, Amin. (2010) step-by-step computer hacking training, Tehran: Taherian Publications.

[5] De Pierre, Mahmoud; Kasabi, Mozhgan (2022), investigating security challenges and how to deal with them in software-based networks.

[6] Javadzadeh, Mohammad Ali; Kangavari, Mohammadreza; Fathi, Seyyed Javad (2013), design and construction of expert system knowledge base for network security test.

[7] Giveei, Mohammadreza and Karmi, Qasim (2013), Application of virtualization in improving the security and reliability of SCADA software and power grid automation.

[8] Ghafarpour, Reza; Poormousa, Ali Asghar and Ranjbar, Ali Mohammad (2014), presenting a criterion for assessing the security of the power grid using fuzzy logic theory.

[9] Asgarian Abianeh, Hossein et al. (2009), Planning the development of the transmission network under the conditions of the electricity market, taking into account the cost of establishing security.

[10] Sattari, Mohammad Ali et al. (2012), using artificial neural networks in information security risk evaluation.

[11] Wu Kehe; Zhang Tong; Li Wei; Ma Gang(2009), "Security Model Based on Network Business Security", In Proc. of Int. Conf. on Computer Technology and Development, 2009. ICCTD '09, Vol. 1, pp. 577-580.