Afro-Asian Journal of Scientific Research (AAJSR)
المجلة الأفروآسيوية للبحث العلمي (AAJSR)
E-ISSN: 2959-6505
Volume 2, Issue 1, January - March 2024, Page No: 240-244
Website: https://www.aajsr.com
SJIFactor 2023: 3.908 **0.51 :2023 (AIF) معامل التأثير العربي** **ISI 2023: 0.337**

Developing computer information security technology and ways to prevent problems from occurring

Abdulssalam Jomah Akroma *[1], Fatimah Allafi Abdullah Isdayrah [2]
[1] Department of Computer Science, College of Science, Bani Waleed University, Libya
[2] Department of Computer Science, College of Education, Bani Waleed University, Libya

*Corresponding author: abdusalamakrouma@gmail.com

Received: December 13, 2023	Accepted: February 09, 2024	Published: February 12, 2024

Abstract
Computer technology and networks have advanced quickly due to social growth, and from being "rare" to "universal," they are now. However, the ensuing security instability has also grown to be a significant issue when it comes to evaluating people and society. Thus, to construct a computer system quickly and steadily, it is now necessary to investigate and research the challenging issue of how to strengthen computer security defence capabilities. To support the governance business, this paper first examines the fundamentals of information security, clarifies associated problems, and offers recommendations for preventative and measurement techniques based on real-world circumstances.

Keywords: Computer information security, information maintenance, protective measures.

Cite this article as: A. J. Akroma, F. A. A. Isdayrah, "Developing computer information security technology and ways to prevent problems from occurring," *Afro-Asian Journal of Scientific Research (AAJSR)*, vol. 2, no. 1, pp. 240–244, January - March 2024.

تطوير تقنية أمن المعلومات الحاسوبية وطرق منع حدوث المشاكل

عبد السلام جمعة كرومة [1*]، فاطمة اللافي عبد الله اسديرة [2]
[1] قسم الحاسوب، كلية العلوم، جامعة بني وليد، ليبيا
[2] قسم الحاسوب، كلية التربية، جامعة بني وليد، ليبيا

الملخص
لقد تطورت تكنولوجيا الحاسوب والشبكات بسرعة نتيجة للنمو الاجتماعي، ومن كونها "نادرة" إلى "عالمية"، فهي الآن كذلك. ومع ذلك، فقد أصبح عدم الاستقرار الأمني الناتج عن ذلك مشكلة مهمة عندما يتعلق الأمر بتقييم الأشخاص والمجتمع. وبالتالي، من أجل بناء نظام حاسوبي بسرعة وثبات، من الضروري الآن التحقيق والبحث في القضية الصعبة المتمثلة في كيفية تعزيز قدرات الدفاع لأمن الحاسوب. في محاولة لدعم أعمال الحوكمة، تتناول هذه الورقة أولاً أساسيات أمن المعلومات، وتوضح المشكلات المرتبطة بها، وتقدم توصيات بشأن تقنيات الوقاية والقياس بناءً على ظروف العالم الحقيقي.

الكلمات المفتاحية: أمن معلومات الحاسوب، صيانة المعلومات، مقاييس الحماية.

Introduction

The benefit of quick information sharing and exchange over computer networks has facilitated societal growth. Computer network technologies are finding their way into a growing number of disciplines, including politics, the military, education, and more. The society has benefited greatly from these common applications. In addition to enhancing people's quality of life, sharing the quick spread of information content in daily life increases productivity at work and advances the advancement of social and spiritual civilization. To provide analysis and pertinent guidance for computer protection, this article will be combined with other relevant content and computer information security technology [1].

Computers bring unlimited ease to people when they enter every home and business, but they also have many negative repercussions. The negative impacts of the Internet will grow increasingly apparent and severe, particularly in the political, economic, military, and other related spheres. Details on the country's armed forces, finances, politics, and other pertinent spheres. National security will be jeopardized in the case of a security incident when the nation's most valuable secrets are disclosed and the interests are harmed. In light of this, it is even more crucial that we continue to conduct research and analysis on information security and maintenance. There are two categories of definitions for information security: broad and limited. When information security is discussed in a general manner, it mostly pertains to host and network security issues. Although it relates to regulations and management, it does not address computer technology at the application level [2]. The discipline is closely related to one another. Information security, taken narrowly, mostly relates to content about computer technology, which includes cryptography knowledge. Depending on how cybersecurity affects a country's interests—be they social stability, personal, or collective—it will suffer varying degrees of harm and incur various costs. It is evident that enhancing Internet management and lowering security risks is the primary issue facing information security today. People's perceptions of computer security issues are starting to shift more and more regularly. Everyone is becoming more and more aware of difficulties pertaining to information security defense since they are connected to their lives and places of employment. Investigating computer maintenance techniques and information security technologies has important ramifications. In light of the current high-risk computer security environment, I hope that the security maintenance techniques and computer information security technology discussed in this article can offer trustworthy solutions.

The Main Problem of Information Security:

a. Limited Monitoring Capabilities:

Information security monitoring equipment can, however, process and feedback hostile attacks or intentional devastation by hackers in a complicated network environment. But the network environment's diversity and unpredictability also provide hackers and vandals with additional openings and chances. Every attack vector is evolving, and information security vulnerabilities are being updated on a regular basis. Our current information security maintenance capabilities are still relatively limited, and they are unable to play the role of actually ensuring the security of the network environment in real time due to the emergence of new attack methods and the inability of the corresponding security protection system technology to closely follow the trend of change to make a corresponding defence response [3].

b. Poor Access Control Ability:

By employing visitor information verification and control, we can stop illegal invasions by sneak-in users through the security prevention and control system. It's challenging to discern the user identity using this method, even though it has a high verification rate.

c. The Strength of Encryption Technology Needs to be Improved:

A password is typically used as part of a security maintenance computing plan to prevent destructive destruction by hackers or attackers. Information encryption is the primary focus of cryptography research at first. Put simply, prior to the information being about to be released, the pertinent content is transformed from its initial readable condition to an unreadable state. The efficiency of cryptography has led to a rise in algorithmic complexity and difficulty, meaning that the actual operation is virtually impenetrable by adversaries. Put another way, if you grasp it theoretically, then other external elements like time, places, tools, etc. will interfere with the actual operation no matter how complex the operating

rules are Therefore, it is practically hard to crack the actual operation as a result, using programmes connected to cryptography is a safe and scientific decision [4].

Computer Information Security Protection Strategy:

a. National Government Gives Support:

Since computer development is a continual process, technologies for computer security protection should also be updated and enhanced regularly. The national government's assistance, greater capital investment, policy support, and guaranteeing that computer information security protection technology research and research personnel have enough financial and policy support are all necessary for this. The state has put in place various mechanisms to penalize employees who work in computer information security, but there are still some challenges with putting these into practice.

To validate these concerns and provide a solution, the state ought to assemble a qualified team. Only the person implementing the encryption behavior knows how the data can be transformed into a readable state; this information can then be shared with a trustworthy third party, who decrypts and reads it. The advancement of computer technology has also led to complexity in the network environment. Figure 1 displays the visualization of the computer encryption algorithm.

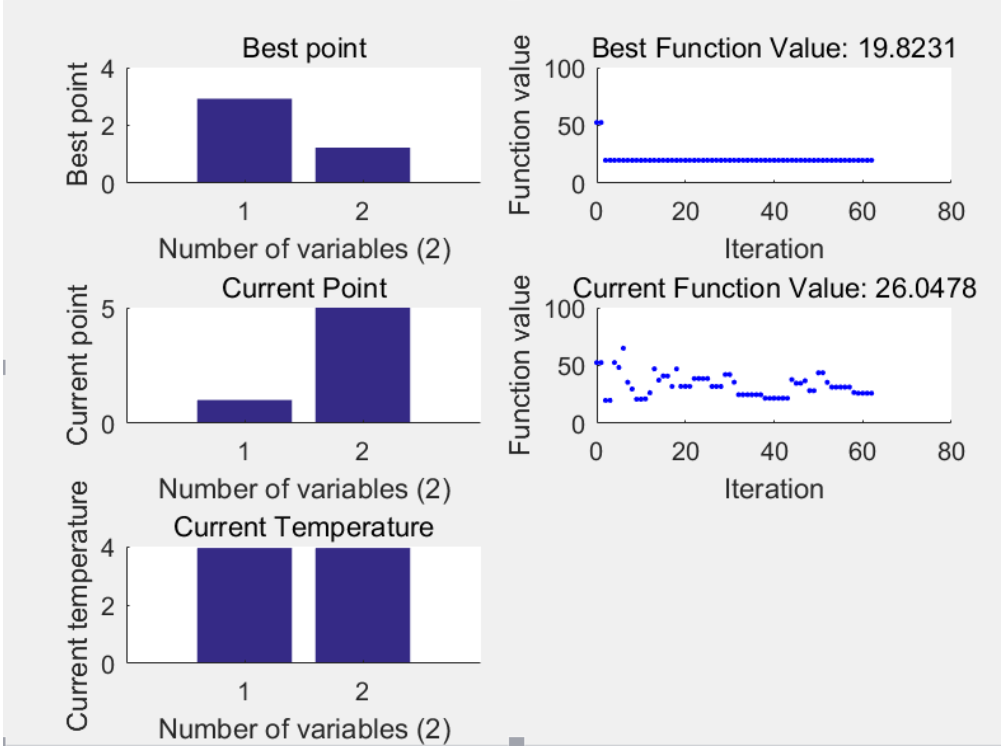

Figure 1: Computer encryption algorithm visualization.

Guarantee the safety of computer data. In addition, instances of computer user rights being violated are becoming increasingly frequent. A lot of people are already familiar with the use of lawful firearms to uphold their rights. Nonetheless, the authorities frequently run across several obstacles when looking into and gathering evidence for these issues. As a result, the national government ought to raise capital expenditure, provide comprehensive training for staff in pertinent fields, and assist in preserving the rights and interests of computer users [5].

b. Find the source of the problem"

Technicians and users need to understand computer information security issues. This means that when computer users find out that information has been stolen, they have to go through specific procedures to get technical help. In addition, regardless of the issue's magnitude or potential for financial loss, technicians ought to investigate the core source of any issues. Take the necessary actions to address computer information security issues in a way that makes sense for the situation. Certain viruses can cause user information leakage or financial loss after they are accessed. These viruses typically take the form of links. Therefore, in order to assist users in getting rid of the infection, experts need look for

issues at their source. In addition, they ought to spread awareness of computer network security issues and create a protective network to address the root of the issue.

c. Improve Information Security Maintenance Technology:
Although computer network technology is updated at a rapid pace, hostile attacks and viruses that pose a threat to computer information security are becoming more sophisticated. In order to do this, the computer technology department must constantly conduct research and development in computer security technology, enhance information security maintenance technology, and safeguard user computer data.

Importance of Developing Computer Information Security Technology:
In today's digital age, computer information security plays a vital role in safeguarding sensitive data and protecting individuals, organizations, and governments from cyber threats. As technology advances, so do the techniques and methods employed by malicious actors seeking to exploit vulnerabilities. Therefore, it is crucial to continually develop and enhance computer information security technology while implementing proactive measures to prevent problems from occurring [6].

1. Evolving Threat Landscape: Cyber threats are becoming increasingly sophisticated, necessitating the continuous development of security technology. Attack vectors such as malware, ransomware, phishing, and social engineering demand robust defense mechanisms that can adapt and respond effectively.
2. Data Breaches and Privacy Concerns: High-profile data breaches have highlighted the need for stronger security measures. Developing advanced encryption algorithms, intrusion detection systems, and access controls is crucial to protect sensitive data and maintain individuals' privacy.
3. Compliance and Regulatory Requirements: Businesses and organizations must comply with various industry-specific regulations and data protection laws. Developing robust security technology helps meet these requirements and avoid legal consequences.

Strategies for Preventing Problems:

1. Regular Software Updates and Patching: Keeping software and operating systems up to date is crucial in addressing known vulnerabilities. Timely installation of security patches can prevent attackers from exploiting weaknesses in the system.
2. Robust Authentication Mechanisms: Implementing strong authentication methods such as multi-factor authentication (MFA) adds an extra layer of security. MFA combines multiple credentials, such as passwords, biometrics, or token-based authentication, significantly reducing the risk of unauthorized access.
3. Employee Awareness and Training: Human error remains a significant factor in security breaches. Regular training programs on best practices, password hygiene, phishing awareness, and social engineering can empower employees to identify and prevent potential threats.
4. Network Segmentation: Dividing a network into smaller, isolated segments reduces the potential impact of a breach. By compartmentalizing sensitive systems and data, organizations can limit lateral movement for attackers and contain potential damage.
5. Encryption and Data Loss Prevention (DLP): Implementing strong encryption protocols ensures that even if data is compromised, it remains unreadable and unusable to unauthorized individuals. DLP solutions can monitor and block sensitive data from leaving the network, mitigating the risk of data leakage.

Developing computer information security technology is an ongoing process that must adapt to the evolving threat landscape. By implementing strategies such as regular software updates, robust authentication mechanisms, employee training, network segmentation, and encryption, organizations can enhance their security posture and reduce the likelihood of successful cyber-attacks. It is crucial for businesses, governments, and individuals to prioritize.

Differs from previous work:
Every means of attack and destruction is changing and information security issues are constantly being updated. However, the emergence of each new attack means and the corresponding security protection

system technology can't closely follow the trend of change to make a corresponding defense response, so our current information security maintenance capabilities are still relatively limited, cannot play the real-time function of ensuring the security of the network environment [3].

Conclusion:

The operating system, computer virus, spyware, malicious assault, and user level are among the threats to computer information security, according to research on computer information security technologies and defence strategies. We cannot implement effective measures until we have a complete understanding of the existing state of computer information security. Information security protection uses computer technology to safeguard the interests of people, companies, and the nation. The backing of the federal government, the disposition of technical staff, and the self-maintenance technologies of individuals and businesses are all necessary for the protection of computer information security. Thus, defenses against these elements need to be reinforced.

Contributions

Research on computer information security technology and protection strategy shows that computer information security is threatened by operating systems, computer viruses, spyware, malicious attacks and user level. Only by fully recognizing the current state of computer information security can we take effective measures. Computer technology information security protection to protect the interests of individuals, businesses and the country. The protection of computer information security depends on the support of the national government, the attitude of technical personnel and the self-maintenance technology of individuals and enterprises. Therefore, protection should be strengthened from these aspects.

References

[1] S. P. Najda, P. Perlin, T. Suski, L. Marona, M. Boćkowski, M. Leszczyński, P. Wisnieski, R. Czernecki, G. Targowski (2016), Advances in AlGaInN laser diode technology for defence, security and sensing applications[P]. Security + Defence.

[2] Shlomi Arnon (2019), Quantum technology for optical wireless communication in data-center security and hacking[P]. OPTO,.

[3] Peng Shen,Xiaoming Ding,Wenjun Ren. Research on Kerberos Technology Based on Hadoop Cluster Security[P]. 2018 2nd International Conference on Advances in Energy, Environment and Chemical Science (AEECS 2018).

[4] Sadeh. Dynamics of the Indian Space Program: Doctrine, Power, Strategy, Security, Policy, Law, Commercialization, and Technology[J]. Astropolitics,2016,14(2-3).

[5] Thomas E. Peterson. Niccolò Scaffai. Il lavoro del poeta. Montale, Sereni, Caproni . Rome: Carocci, 2015. 248 pp.[J]. Symposium: A Quarterly Journal in Modern Literatures,2017,71(3)..

[6] Smith, D. (2020). Computer Security: Principles and Practice (4th edition.). Pearson

[7] Whitman, M. E., & Mattord, H. J. (2019). Principles of Information Security (6th ed.). Cengage Learning.

[8] Scarfone, K., & Souppaya, M. (Eds.). (2013). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST).