საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 15, №2, 2021
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 15, no. 2, 2021

Informatics

Use of Wireless Networks in Reference-Legal Systems and Information Security Ensurance

Ioseb Kartvelishvili*, Luka Shonia*, Saba Kvesitadze*

*Georgian Technical University, Tbilisi, Georgia

(Presented by Academy Member Ramaz Khurodze)

The paper presents integrated automated systems for managing normative-legal documents and business processes in state institutions and private structures using wireless networks and protecting them from any accidental and deliberate interference in the normal functioning of the process, attempted theft of information, modification or physical destruction of its components. The Paper also introduces the possibility of neutralizing various alarm impacts and the need to ensure safety. It presents the components and systems of wireless local area networks, provides with the most common forms of threats associated with the use of wireless LAN components, and each is characterized by its own characteristics. A new approach has been developed to increase the security of routing in wireless LAN. In addition, the wireless LAN is schematically represented, using an authentication server and specific connections between network devices. *© 2021 Bull. Georg. Natl. Acad. Sci.*

Reference-legal systems, normative-legal documents, wireless networks, information security

The solution of modern problems of community management is increasingly associated with the development of information processes. Information, media, methods and technologies, as well as their processing processes are perceived as an integral part of society. Today, computerization processes are actively involved in almost all areas of human activity. In this regard, reference-legal systems are not the exclusion with its processes of collection, storage, processing and use of normative-legal documents, i.e the formation, interpretation and communication of legal information. Solving modern problems, managing society is increasingly linked to the development of information processes. Information, media, their processing and use methods (technologies) have become an integral part of public relations.

The colossal volume of legislative information and the dynamics of its changes require the use of modern methods and tools from lawyers, businessmen and any stake holders in the process of working with legal information. At present, such tools are reference-legal systems, the main task of which is to promptly provide accurate legal information to an indefinite number of users in state institutions or private structures. One of the main purposes of the reference-legal system is to form appropriate legal information in the process of

making important decisions, to provide the user with reliable and complete normative and other information easily and operatively. In addition, it is also necessary to develop information security issues. Information security means the protection of society's information environment, which ensures the formation, use and development of information in accordance with the interests of citizens, society and the state. The prevention and elimination of information security threats is based on the development and implementation of protection mechanisms and means. These can be organizational, technical, programmatic, social, legal and other mechanisms. Information security issues concern both the entities whose interests and rights are protected and the entities that provide such protection [1].

Main Part

Recently, security and quality of service in computer networks (wired and wireless) have become the subject of highly important and active research due to the growing demand for data packet support. Without adequate security, organizations avoid using computer networks. Security issues in computer networks are a significant obstacle to the widespread adaptation of such networks. Consequently, the security of such computer networks is an important area that needs to be addressed if such networks are to be widely used. It is essential that researchers in this field identify open problems and provide appropriate solutions to those problems.

Security is an extremely important issue for wireless networks as communication signals spread across the environment are available to capture. Therefore, companies and individual consumers should be aware of potential problems and take appropriate action. Any system that needs protection has its weaknesses or shortcomings, and the attacker chooses part or all of it as an object of attack. Consequently, one of the approaches to creating system security mechanisms is to discuss the threats and potential attacks facing the system, given that the system has flaws. Security mechanisms must ensure the security of the system in the face of given threats, attacks and vulnerabilities [2].

It should be noted that computer network routing protocols do not specify any preventive measures or security mechanisms in the specifications. Thus, the security of wireless network routing protocols has become an urgent necessity to stimulate and expand the scope of network launch.

In modern conditions, the creation of effective mechanisms for the management of information resources of legal-search automated systems in state institutions and private structures is impossible without the scientific substantiation of information security and the practical implementation of a balanced policy. These institutions store and process a large amount of various data related not only to the conduct of their activities, but also to the implementation of various research and construction projects, personal data processing, storage of state commercial, personal and other confidential information [1].

The increase in crimes in the field of high technology has led to demands on the legal-search systems of state and private institutions for the protection of computing network resources. The need to create its own security system has become urgent, which means the existence of a legal-normative base, the formation of a security concept, the development of special measures, the planning of security procedures, design, the implementation of technical means of information protection. All of the above system components define a single information security policy.

Wireless LANs fully meet the requirements for wireless connectivity to establish a connection within a building. Wireless LANs are made up of the same components as traditional LANs. Their protocols are also similar. The only difference is that the use of wires is not necessary when setting

up wireless LANs. Wireless LAN users work with many devices - PCs, laptops, etc. Using wireless LANs to connect devices to each other is effective for personal computers because it excludes the need to lay wires.

The main components of a wireless LAN are: the network interface radio plate, access points, routers, and repeaters. The network interface radio plate is implemented on the 802.11 standard. These radio plates usually operate on one physical level - 802.11a or 802.11b/g. The radio plate, which is integrated with the wireless LAN, must realize the standard version. Wireless LAN radio plates, which provide and realize different versions of this standard and have a high level of interoperability, are becoming more and more widespread.

The access point consists of a radio plate that provides a connection between a separate consumer device of the wireless local area network and a wired board of the network interface that provides interaction with the distributed system. Access point system software enables the interaction between wireless LAN parts and a distributed access point system. This software differentiates access points by the degree of management and security features provided [3].

The router, judging by the name, transmits the information packets from one network to another, choosing the next best channel to deliver the packet to the nearest point. Routers use Internet Protocol (IP) packet titles and routing tables. Internal protocols are also used to determine the best path for transmitting each packet. A typical wireless LAN router has 4 ports, so it can also serve as a print server. All of this allows wireless network users to receive and send packets across multiple wired networks as if they were connected to one of them.

Routers use network address translation (NAT) protocols, which allow many network devices to share a single IP address provided by an Internet service provider (ISP). Routers also use the dynamic host configuration protocol (DHCP) for all device services, allowing each device to submit separate IP addresses. Together, NAT and DHCP enable multiple network devices (such as PCs, laptops, and printers) to operate on the Internet using a single IP address [1].

The repeater, in the existing network infrastructure, simply regenerates the signals that propagate through the network to extend the range. The wireless LAN repeater has no physical contact with any part of the network. It receives radio signals from the access point and re-transmits the received data frames. All of this allows the repeater, which is located between the access point and the removed user, to function as a frame retransmitter that transmits from the user to the access point and vice versa. Therefore, wireless repeaters are an effective solution to the problem of attenuation of signals caused by radio failures.

Security for wireless LANs is an extremely important issue as communication signals spread across the environment are available to capture. Therefore, companies and individual consumers should be aware of potential problems and take appropriate action. Any system that needs protection has its weaknesses or shortcomings, and the attacker chooses part or all of it as an object of attack. Consequently, one of the approaches to creating system security mechanisms is to discuss the threats and potential attacks facing the system, given that the system has flaws. Security mechanisms must ensure the security of the system in the face of given threats, attacks and vulnerabilities.

For example, any malicious person using various software tools can easily find vulnerable packets on the wireless network and completely open the data contained in it. For example, outsiders who are several hundred meters away from the building where the wireless LAN operates will be able to find all the transactions that take place in the wireless network. Of course, the main danger lies in the fact that as a result of attacks someone can get access to such important

information as usernames and passwords, credit card numbers and more.

Similarly, anyone in the vicinity of the building can, without any effort, monitor the systems in the wireless LAN if no precautions are taken. For example, someone in a car parked near a building may be able to access one of the base stations in the building. If the necessary protection measures are not taken, such a person can infiltrate the server and systems that end up in the corporate network. Unfortunately, most companies use a base station configuration when setting up wireless networks, which is installed from the beginning and fails to provide the necessary security measures, which predetermines seamless interaction with the systems server [4].

The use of authentication and encryption mechanisms increases the security of wireless networks, but experienced hackers are looking for vulnerabilities, knowing how the network protocols work. The hacker places a fictitious device between legal users and the wireless network. For example, the standard "human in the middle" type attack uses the Address Resolution Protocol (ARP), which is used on all TCP/IP (Transmission Control Protocol/Internet Protocol) networks. A hacker armed with the necessary software tools can establish control over a wireless network using ARP. Denial of Service (DoS) Attack - This is an attack that renders a wireless network unusable or blocked. The possibility of such an attack should be considered by anyone who even operates a wireless network. It is necessary to think about what will happen when the network becomes inaccessible indefinitely. The severity of a DOS attack depends on what results from the failure of the wireless network [1].

Wireless LANs, unlike conventional networks, have an increased risk factor for attacks due to the following main reasons: wireless LANs do not have a filter, which can be used to protect against attacks. There is no server that is characterized by an increased trust factor; wireless networks are characterized by the constant movement of objects and at the same time there are no physical channels. In the absence of these channels, information is

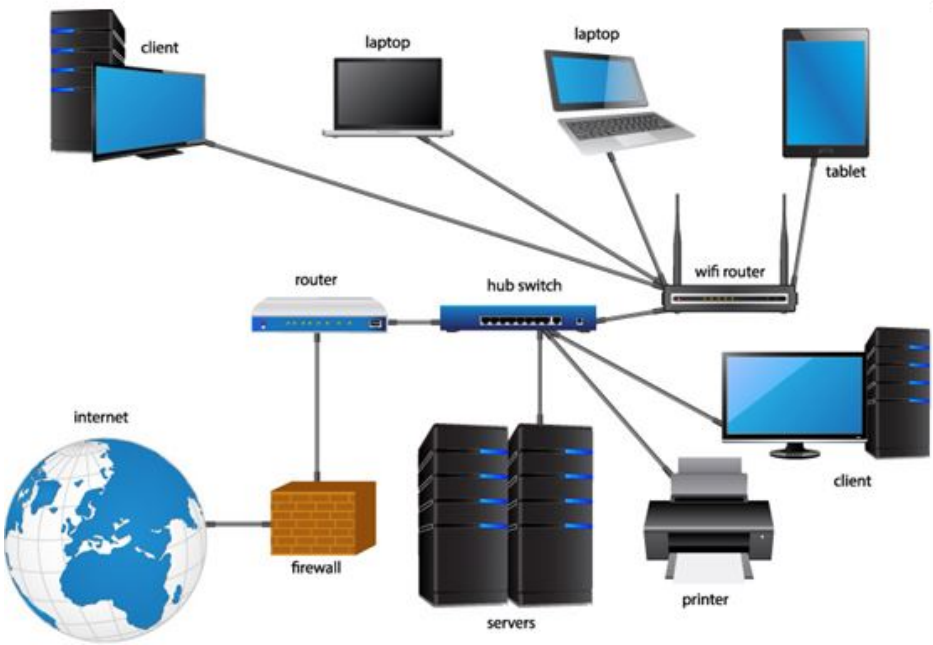

Fig. 1. Wireless LAN which uses authentication server and specific connections.

transmitted over the air, which itself is also a danger, since attacks start precisely from listening to the channel [4].

Based on the above problems, a new approach has been developed to increase the security of wireless routing in the local area network. In a wireless LAN it is necessary to use an authentication server, which will allow to monitor the connection processes between network devices and write them to the database. It is also necessary to use two-way authentication between network devices, thanks to which it is possible to solve many problems related to security. In two-way authentication, the wireless user and the wireless network prove their identities to each other.

In private companies or enterprises, the wireless local area network should preferably consist of several access points and a wired router. A combination of an access point and a wired router can replace a wireless LAN router, and this is a less expensive solution than purchasing a wireless LAN router [3]. It is also essential that several wireless users (computers or laptops) are connected to any particular access points and that access points are not accidentally retrieved while transmitting information. Also, IP addresses should be prescribed individually on all network devices by the network administrator and under no circumstances should IP addresses be randomly provided to local network users using the DHCP protocol (Fig. 1).

Most often wireless LANs are created in compliance with the 802.11 standard. The IEEE 802.11 standard describes a common access management protocol in the transmission area (Media Access Control (MAC)) and several physical levels of wireless LANs. The IEEE 802.11 Standard Development Working Group is actively working to improve the features and security of wireless LANs. Every network device has its own unique MAC address, and two-way authentication must be performed to verify the identity of devices before transmitting information by verifying it and IP addresses [4].

Conclusion

In the period of technological innovations, when the direction is experiencing rapid development, it is necessary to facilitate the process of continuous updating of the security of the legal-search system. This is the task that automated legal-search systems of state and private institutions are constantly facing. In practice, the continuous work cycle is subject to the strengthening of protection mechanisms and the introduction of even more innovative methods. In turn, the development of the latest methods and ideas and their practical application, will clearly show the advantages and disadvantages of the method. Based on situational analysis, the methods shall be strengthened in different directions and the protection methods for the present moment shall be further improved.

ინფორმატიკა

საცნობარო-სამართლებრივ სისტემებში უსადენო ქსელების გამოყენება და ინფორმაციული უსაფრთხოების უზრუნველყოფა

ი. ქართველიშვილი*, ლ. შონია*, ს. კვესიტაძე*

საქართველოს ტექნიკური უნივერსიტეტი, თბილისი, საქართველო

(წარმოდგენილია აკადემიის წევრის რ. ხუროძის მიერ)

ნაშრომში წარმოდგენილია სახელმწიფო დაწესებულებებსა და კერძო სტრუქტურებში ნორმატიულ-სამართლებრივი დოკუმენტების მართვისა და საქმიანი პროცესების ინტეგრირებული ავტომატიზებული სისტემები უსადენო ქსელების გამოყენებით და მათი დაცვა მისი ნორმალური პროცესის ფუნქციონირებაში შემთხვევითი და მიზანმიმართული ჩარევისაგან, ინფორმაციის მოპარვის მცდელობისაგან, მისი კომპონენტების მოდიფიცირებისა ან ფიზიკური განადგურებისაგან, სხვადასხვა საგანგაშო ზემოქმედების განეიტრალების შესაძლებლობა, უსაფრთხოების უზრუნველყოფის აუცილებლობა. აგრეთვე წარმოდგენილია უსადენო ლოკალური ქსელების კომპონენტები და სისტემები. მოყვანილია უსადენო ლოკალური ქსელების გამოყენებასთან დაკავშირებული საფრთხეების ყველაზე გავრცელებული ფორმები და თითოეული მათგანი დახასიათებულია თავისი თვისებებით. უსადენო ლოკალურ ქსელში მარშრუტიზაციის უსაფრთხოების ამაღლების მიზნით შემუშავებულია ახალი მიდგომა. სქემატურად წარმოდგენილია უსადენო ლოკალური ქსელი, სადაც გამოყენებულია აუტენტიფიკაციის სერვერი და ქსელურ მოწყობილობებს შორის კონკრეტული შეერთებები.

REFERENCES

1. Shonia O., Kartvelishvili I., Kolbaia L. (2014) Development of Automated System for Managing Normative-Legal Documents and Business Processes and Ensuring Security. GTU, Automated Management Systems #1 (17), Tbilisi.
2. Shonia O., Nareshelashvili G., Kartvelishvili I. (2018) Wireless network security. Georgian Technical University, Tbilisi.
3. Shonia L. (2020) Methods for ensuring multi-level security of a corporate network And means research. Tbilisi.
4. Prangishvili A., Rodonaia I., Shonia O. (2017) Process of wireless local area networks monitoring. International *Journal of Transportation Systems.*

Received May, 2021