International Journal of Culture and Modernity
ISSN 2697-2131, **Volume 25 | Fab-2023**
https://ijcm.academicjournal.io

Security Level in the Domestic Local Area Network

Otakulov Oybek Hamdamovich
Candidate of Technical Sciences, Associate Professor, Fergana Branch of Tashkent
University of Information Technologies Named After Muhammad Al-Khorezmi

Mirzayev Muhammadjon
Fergana Branch of Tashkent University of Information Technologies
Named After Muhammad Al-Khorezmi 2nd Master of Occupation

ANNOTATION

This article provides ideas on how to organize the network system and its security. As the most basic issue, the local network is covered.

KEYWORDS: LAN, Ethernet technology, NASA, client/server, wardriving, WPA, WPA2, and WPA3.

A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.

The rise of virtualization has also fueled the development of virtual LANs, which enable network administrators to logically group network nodes and partition their networks without a need for major infrastructure changes.

For example, in an office with multiple departments, such as accounting, IT support, and administration, each department's computers could be logically connected to the same switch but segmented to behave as if they are separate.

The advantages of a LAN are the same as those for any group of devices networked together. The devices can use a single Internet connection, share files with one another, print to shared printers, and be accessed and even controlled by one another.

LANs were developed in the 1960s for use by colleges, universities, and research facilities (such as NASA), primarily to connect computers to other computers. It wasn't until the development of Ethernet technology (1973, at Xerox PARC), its commercialization (1980), and its standardization (1983) that LANs started to be used widely.

While the benefits of having devices connected to a network have always been well understood, it wasn't until the wide deployment of Wi-Fi technology that LANs became commonplace in nearly every type of environment. Today, not only do businesses and schools use LANs, but also restaurants, coffee shops, stores, and homes.

Wireless connectivity has also greatly expanded the types of devices that can be connected to a LAN. Now, nearly everything imaginable can be "connected," from PCs, printers, and phones to smart TVs, stereos, speakers, lighting, thermostats, window shades, door locks, security cameras--and even coffeemakers, refrigerators, and toys.

In general, there are two types of LANs: client/server LANs and peer-to-peer LANs.

A client/server LAN consists of several devices (the clients) connected to a central server.

The server manages file storage, application access, device access, and network traffic. A client can be any connected device that runs or accesses applications or the Internet. The clients connect to the server either with cables or through wireless connections.

Typically, suites of applications can be kept on the LAN server. Users can access databases, email, document sharing, printing, and other services through applications running on the LAN server, with read and write access maintained by a network or IT administrator. Most midsize to large business, government, research, and education networks are client/server-based LANs.

A peer-to-peer LAN doesn't have a central server and cannot handle heavy workloads like a client/server LAN can, and so they're typically smaller. On a peer-to-peer LAN, each device shares equally in the functioning of the network. The devices share resources and data through wired or wireless connections to a switch or router. Most home networks are peer-to-peer.

In today’s connected world, almost everyone has at least one internet-connected device. With the number of these devices on the rise, it is important to implement a security strategy to minimize their potential for exploitation (see Securing the Internet of Things). Internet-connected devices may be used by nefarious entities to collect personal information, steal identities, compromise financial data, and silently listen to—or watch—users. Taking a few precautions in the configuration and use of your devices can help prevent this type of activity.

What are the risks to your wireless network?

Whether it’s a home or business network, the risks to an unsecured wireless network are the same. Some of the risks include:

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

War driving

War driving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is known as “wardriving.”

Evil Twin Attacks

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker’s system, it’s easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

Unauthorized Computer Access

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks, you deny sharing files and folders. Only allow sharing on recognized home networks and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device's files.

Shoulder Surfing

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors that prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

Theft of Mobile Devices

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft is important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or personal identification number (PIN). In addition to encrypting device content, it is also advisable to configure your device's applications to request login information before allowing access to any cloud-based information. Last, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device.

What can you do to minimize the risks to your wireless network?

Change default passwords. Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device. (See Choosing and Protecting Passwords.)

International Journal of Culture and Modernity

ISSN 2697-2131, **Volume 25 | Fab-2023**

https://ijcm.academicjournal.io

Restrict access. Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the "guest" account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.

Encrypt the data on your network. Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.

Protect your Service Set Identifier (SSID). To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device's SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

Install a firewall. Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls for Home and Small Office Use).

Maintain antivirus software. Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware (see Protecting Against Malicious Code and What is Cybersecurity?).

Use file sharing with caution. File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing (see Choosing and Protecting Passwords).

Keep your access point software patched and up to date. The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.

Check your internet provider's or router manufacturer's wireless security options. Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.

Connect using a Virtual Private Network (VPN). Many companies and organizations have a

VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

References

1. Parpieva Odinakhon Rakhmanovna, Muydinova Yoqutkhon Giyaziddinovna, Safarova Gulora Maxammadievna //BREAST CANCER// ACADEMICIA: An International Multidisciplinary Research Journal. Vol. 11, Issue 11, November 2021. 489-492 page.
2. O.Parpiyeva, A.Ostonaqulov //Psychology of patients with oncological diseases// International Scientific Journal ISJ Theoretical & Applied Science 06 (74) 2019. Philadelphia, USA. 642-645 page.
3. O.R.Parpieva, E.Muydinova, G.Safarova, N.Boltaboeva //Social and psychological aspects of a healithy life style// ACADEMICIA: An International Multidisciplinary Research Journal.Vol. 10, Issue 11, November 2020. 1364-1368 page.
4. Parpieva Odinakhon Rakhmanovna, Ostanaqulov Alijon Dadajon Ugli, //Modern Scientific Research In Oncological Diseases //The American Journal of Medical Sciences and Pharmaceutical Research, 3(03), (2021).117-121page
5. Parpieva Odinakhon Rakhmanovna, Ostanaqulov Alijon Dadajon Ugli, //Mental-emotional Disorders in Patients with Oncological Disiases// EPRA International Journal of Multidisciplinary Research (IJMR). Volume: 7/ Issue: 4/ Aprel 2021. 232-235 page.
6. O.Parpiyeva, A.Ostonaqulov //Drugs to treat the psychological state of the patients and their methods// Международном научно-практическом журнале “Экономика и социум” Электронное научно-практическое издание. Выпуск №1 (56) – 2019. 93-97 стр
7. Parpiyeva O.R, Marifjonovna B.N //The effect of harmful habits on human health// Международный научно-практический журнал “Мировая наука” Выпуск №5(26) – 2019. 76-79 стр
8. O.R.Parpiyeva, Ostanaqulov A.D //SCHIZOPHRENIA DISEASE// Международный научно-практический журнал “Теория и практика современной науки” Выпуск №6 (48) – 2019. 18-21 стр
9. O.R.Parpiyeva, Ostanaqulov A.D //Thoughts that do not go away from the brain// Международный научно-практический журнал “Мировая наука” Международное научное издание. Выпуск № 6 (27) – 2019. 9-12 стр
10. Parpiyeva O.R, Raimjonova Kh.G. qizi //The role of a nurse in patient care// Международный научно-практический журнал “Мировая наука” Международное научное издание. Выпуск № 11(32) – 2019. 56-59 стр
11. ogli Melikuziev, A. L. (2022). HISTORICAL AND MODERN CLASSIFICATION OF PARALINGUISTICS. Academicia Globe: Inderscience Research, 3(10), 126-128.
12. Parpiyeva O.R, Jamoliddinova U. A. Qizi //PROTECTION OF THE HEALTH OF CHILDREN AND ADOLESCENTS// Международный научно-практический журнал “Мировая наука” Международное научное издание. Выпуск № 11(32) – 2019. 53-55

стр

13. Parpieva O.R. Solieva Z.A. //THESE IMPORTANT THANKS// Международный научно-практический журнал “Теория и практика современной науки” Выпуск №4 (34) – 2018. 85-87 стр
14. Парпиева О.Р. Болтабоева Н.М. //ЭТАПЫ РЕШЕНИЯ ПЕДАГОГИЧЕСКОЙ ЗАДАЧИ// Международный научно-практический журнал “Теория и практика современной науки” Выпуск №6 (48) – 2019. 388-390 стр
15. Parpiyeva O.R. Ostanaqulov A.D. // HEALTH THEORY// Международный научно-практический журнал “Форум молодых ученых” Вып №6 (34) 2019. 26-29 стр
16. Ostanakulov A.D The history and role of Islam and psychology in the education system in Central Asia. Research Jet Journal of Analysis and Inventions https://RESERCHJET.ACADEMIASCIENCE.ORG ISSN: 2776-0960 Impact Factor: 7.655 VOLUME 2, ISSUE 4, APRIL - 2021
17. Soliev F. S., Muminov D. To determine individual specificity and hidden potential of the personality according to external signs of behavior //ACADEMICIA: An International Multidisciplinary Research Journal. – 2021. – Т. 11. – №. 5. – С. 1258-1265.