Lecture 10

Securing the Network Infrastructure

Securing the Network Infrastructure

- Introduction to Network Infrastructure Security
- Securing the Switch
- Securing the Router

Introduction to Network Infrastructure Security

- **Network infrastructure** refers to all the resources of a network that make network or internet connectivity, management, business operations, and communication possible.
  - Network infrastructure allows for effective communication and service between users, applications, services, devices, and so forth.
- **Network security** is any activity designed to protect the **usability and integrity** of your network and data. It includes both hardware and software technologies.
  - It targets a variety of threats. It stops them from entering or spreading on your network. Effective network security manages access to the network.

5 Critical Steps for Securing a Network Infrastructure

1. **Running a Network Security Audit.**
2. **Conduct Cybersecurity Awareness Training**
3. **Limit User Access Privileges to the Minimum Necessary for Work.**
4. **Patch Your Software**
5. **Review Your Cybersecurity Tools.**

Ref: https://www.compuquip.com/blog/securing-network-infrastructure

Running a **Network** Security Audit

- A comprehensive audit covers multiple review processes, such as:
  - **Firewall Architectures/Configurations.** What kind of firewall solutions are in place and where do they rest on your network (at the perimeter, in between individual servers/assets)? Also, are firewall configurations up to date and free of conflicts that could be exploited by an attacker?
  - **Asset Identification.** What kind of assets are on the network, and what kinds of software and operating system (OS) does each one run? Knowing what's on your network is crucial for identifying potential weaknesses so they can be fixed—such as software that isn't up to date with its latest security patch.
  - **Security Policies/Procedures.** What standards does each of the people in your organization understand/follow when it comes to keeping your business' data secure? Do you have a BYOD (bring-your-own-device) policy for using personal devices at work? How are security policies enforced? A review of all your security policies and procedures is crucial for keeping your data secure.
  - **Risk Assessment.** After identifying all of the assets on your network and reviewing your security policies/procedures, what are the most significant threats that you need to take care of ASAP? Risk assessments help you prioritize your cybersecurity efforts to close your biggest gaps first.
- This kind of cybersecurity audit is a crucial first step in securing a network infrastructure against potential intrusion attempts because it allows you to identify critical gaps in your security architecture so you can fix them. It can also help you to prioritize which of the following next few steps you need to focus on first based on the risks you've identified.

Conduct Cybersecurity Awareness Training

- The biggest weak link in any organization's cybersecurity architecture is, usually, the organization's employees. Employees who aren't aware of the various threats found online may end up falling for phishing attacks, downloading viruses to their workstations, or using easy-to-guess passwords that let others hijack their user accounts.
- Cybersecurity awareness training helps to plug the biggest gaps in your workforce's knowledge—letting them know what the risks are and how to identify some basic phishing attempts. This can help harden the human element of your workforce against online attacks.
- According to data cited by the Harvard Business Review, "60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors." Considering this, providing cybersecurity awareness training can help curtail a significant portion of cyberattacks.

Limit User Access Privileges to the Minimum Necessary for Work

- If three-quarters of insider attacks are malicious, or carried out purposely by users with legitimate access, how can your organization prevent such attacks or limit their impact? One solution is to apply **a policy of least privilege (POLP)** to every user account on the network.
- Under a POLP, users on the network are restricted to having only the minimum level of access that they need to perform their core job function. The major benefit of this is that it helps to dramatically reduce the risk of an insider stealing data—especially if your network assets are strictly isolated from one another.
- By limiting access, you can limit the amount of data an employee can compromise without having to breach other defenses—which gives your intrusion detection system (IDS) more of a chance to detect the abnormal activity.

Patch Your Software ASAP

- **Another major security vulnerability is unpatched software on the network. Companies are constantly finding and fixing security flaws in their software and systems—flaws that give hackers a way past otherwise solid defenses.**
- **Example, the "zero-day" exploit Microsoft software."**
- **So, one of your top priorities after a security audit is to look at the list of software on each of your network assets and make sure that they all have the most recent security patches—especially if the software version is years out of date. If you have software that is no longer supported by the original developer, it may be time to uninstall that software and replace it with a newer program that has up-to-date protection.**

* Zero-day A zero-day vulnerability is a computer-software vulnerability that is unknown to those who should be interested in mitigating the vulnerability.

Review Your Cybersecurity Tools

- Does your organization have the right tools in place to sufficiently mitigate your network's cybersecurity risks? While you don't have to pick up every cybersecurity tool on the market to protect your business' network infrastructure, you should at least cover the basics needed for mitigating risks and covering the regulatory obligations specific to your industry.
- compiled a list of the various assets on your network—including the individual cybersecurity tools on the network (firewalls, IDS/IPS, antivirus, remote backups, etc.) that you can use to respond to your biggest threats.

Physical Security Controls

- **Physical security controls are those controls pertaining to the physical infrastructure, physical device security, and physical access.**
- **Physical Network Infrastructure**
  - **The physical network infrastructure encompasses both the selection of the appropriate media type and the path of the physical cabling (the network topography).**
  - **You want to ensure that no intruder is able to eavesdrop on the data traversing the network and that all critical systems have a high degree of availability.**

Ref: Cisco.Press.Designing.Network.Security_ebook

Physical Media Selection

- From a security point of view, the type of cable chosen for various parts of the network can depend on the sensitivity of the information traveling over that cable.
- The three most common cable types used in networking infrastructures are twisted pair, coax, and optical fiber.
- Optical fiber is most often used in high-bandwidth and long-haul environments. Unlike either twisted pair or coax, optical fiber does not radiate any energy and, therefore, provides a very high degree of security against eavesdropping.
- Optical fiber is also much more difficult to tap into than either twisted pair or coax cable. Wiretaps can sometimes be detected by using tools to measure the physical attenuation of cable.
- Typically, a time-domain reflectometer (TDR) tool is used to check coax cable, and an optical time-domain reflectometer (OTDR) tool is used for optical fiber cable. These devices are used mainly to measure signal attenuation and the length of an installed cable base; sometimes, however, they can also detect illegal wiretaps

Ref: Cisco.Press.Designing.Network.Security_ebook

Network Topography

- **The physical path of the media, also known as the network topography, is a concern for the availability of the network and its attached devices. It touches on the reliability and security of the infrastructure. It is important to have a structured cabling system that minimizes the risk of downtime.**
- **The cable infrastructure should also be well secured to prevent access to any part of it. If cables installed between buildings are buried underground, they must be buried a minimum of 40 inches, although local regulations might dictate other guidelines. Sometimes, cables can be encased in concrete to provide maximum protection.**
- **The International Telecommunication Union has a number of recommendations (the Series L Recommendations) that cover the construction, installation, and protection of cable plants**

Ref: Cisco.Press.Designing.Network.Security_ebook

Physical Device Security

- **Physical device security is sometimes understated.**
- **Intruders with enough incentive will think of anything to get at what they want.**
- **Physical device security includes identifying the location of the devices, limiting physical access, and having appropriate environmental safeguards in place.**

Ref: Cisco.Press.Designing.Network.Security_ebook

Physical Device Security: Physical Location

- **The location of critical network resources is extremely important. All network infrastructure equipment should be physically located in restricted access areas to eliminate the possibility of unauthorized access by physical proximity.**
- **Facility issues can be a horrific nightmare, but when it comes to creating space for wiring closets that house critical infrastructure equipment, such as switches, firewalls, modems, and routers, it is imperative that you fight for whatever autonomous space there is.**
- **Don't overlook any aspect of the physical facility.**
- **Having a secure lock on a wiring closet does not provide much protection if you can go through the ceiling panels to get into the room**

Ref: Cisco.Press.Designing.Network.Security_ebook

Physical Device Security: Physical Location

- **The infrastructure equipment includes more than just the networks and the routers, firewalls, switches, and network access servers that interconnect the networks. Infrastructure equipment also includes the servers that provide the various network services:**
- **Network management (SNMP)**
- **Domain Name Service (DNS)**
- **Network time (NTP)**
- **Network File System (NFS)**
- **HyperText Transfer Protocol (HTTP)**
- **User authentication and authorization (TACACS+, RADIUS, Kerberos) • Network audit and intrusion detection**

Ref: Cisco.Press.Designing.Network.Security_ebook

Physical Device Security: Physical Access

- **Who has access to the wiring closets and restricted locations?**
- **The physical access requirements of controlled areas are determined largely by the results of the risk analysis or a physical security survey.**
- **It is good practice to restrict physical access to wiring closets and locations of critical network infrastructure equipment.**
- **Access to these areas should not be permitted unless the person is specifically authorized or requires access to perform his or her job.**
  - **Note The following is a true story. Although it might represent a rare occurrence, it is best to avoid any such instances if possible. A network connection was down, and some resources were unavailable. After some time spent analyzing possible problems, the equipment closet was inspected. It turns out that the cable connecting the LAN to the router had been disconnected.**
  - **A maintenance worker had been working in another part of the closet, found the wire to be in the way, and disconnected it. When his work was finished, he forgot to reconnect it. A more devious example is that of a competitor posing as a maintenance worker and gaining access to confidential information.**

Ref: Cisco.Press.Designing.Network.Security_ebook

Physical Device Security: Physical Access

- Part of the physical security policy should be to have contract maintenance personnel or others who are not authorized with unrestricted access, but who are required to be in the controlled area, to be escorted by an authorized person or to sign in before accessing the controlled area.
- To ensure an enforceable physical security policy, it is essential to ensure that people's work areas mesh well with access restrictions.
- If these conditions are not met, well-meaning employees will find ways to avoid your physical security (for example, they will jam doors open rather than lock and unlock them 15 times per hour).
- If your facility is providing temporary network access for visitors to connect back to their home networks (for example, to read e-mail), plan the service carefully. Define precisely where you will provide it so that you can ensure the necessary physical access security.
- A typical example is at large industry meetings; if these meetings are hosted at a corporate facility, the host corporation usually has a network for guests. This network should reside in a single area and access should be given only to conference attendees.

Ref: Cisco.Press.Designing.Network.Security_ebook

Physical Device Security: Environmental Safeguards

- **Adequate environmental safeguards must be installed and implemented to protect critical networked resources. The sensitivity or criticality of the system determines whether a security is "adequate." The more critical a system, the more safeguards must be put in place to ensure that the resource is available at the Design and Implementation of the Corporate Security Policy.**
- **At a minimum, you should consider the following environmental safeguards: • Fire prevention, detection, suppression, and protection • Water hazard prevention, detection, and correction • Electric power supply protection • Temperature control • Humidity control • Natural disaster protection from earthquakes, lightning, windstorms, and so on • Protection from excessive magnetic fields • Good housekeeping procedures for protection against dust and dirt**

Ref: Cisco.Press.Designing.Network.Security_ebook

Logical Access Control

- **Access to equipment and network segments should be restricted to individuals who require access.**
- **Two types of controls should be implemented:**
  - **Preventative controls, which are designed to uniquely identify every authorized user and to deny access to unauthorized users.**
  - **Detective controls, which are designed to log and report the activities of authorized users and to log and report unauthorized access or attempted access to systems, programs, and data.**

Ref: Cisco.Press.Designing.Network.Security_ebook

Authentication Assurance

- **Some organizations still base their authentication mechanisms on standard, reusable passwords. Any reusable password is subject to eavesdropping attacks from sniffer programs.**
- **Choose passwords that cannot be guessed easily. Many automated password-cracking programs Design and Implementation of the Corporate Security Policy] use a very large dictionary and can crack passwords in a matter of seconds.**
- **Passwords should also be as long as the system supports and as users can tolerate. Change default passwords immediately when you install new network infrastructure equipment. Don't forget to change the passwords for console access and passwords used for maintenance purposes. For any product you buy, find out from the manufacturer whether there are ways to recover passwords and whether there are any ways to access configurations using these passwords (usually through undocumented means). • Restrict access to the password when possible. Many vendors now have features that encrypt the password portion of configuration files. Use these features whenever they are available. • Provide guidelines for how often a user should change his or her password. It is recommended that passwords be changed at least whenever a privileged account is compromised or when there is a critical change in personnel.**

Ref: Cisco.Press.Designing.Network.Security_ebook

Passwords guidelines

- **Choosing Passwords Here are some guidelines for choosing appropriate passwords:**
  - **Do not use your login name in any form (as-is, reversed, capitalized, doubled, and so on).**
  - **Do not use your first, middle, or last (current or former) name in any form. Do not use any of your immediate family's names (spouse, offspring, parents, pets, and so on).**
  - **Do not use other information easily obtained about you, including license plate numbers, telephone numbers, social security numbers, the brand of automobile you drive, the name of the street you live on, and so on.**
  - **Do not use a password of all digits or of all the same letter. These types of passwords significantly decrease the search time for a cracker.**
  - **Do not use a word contained in any English or foreign language dictionaries, spelling lists, or other lists of words.**

Ref: Cisco.Press.Designing.Network.Security_ebook

- **Do not use a password shorter than six characters. Never give your network password to anyone. Securing your password is your responsibility. The whole purpose of having a password in the first place is to ensure that no one other than you can use your logons.**
- **Remember that the best-kept secrets are those you keep to yourself.**
- **Never e-mail your password to anyone. Use a password with mixed-case alphabetics, if possible (some systems use passwords that are case sensitive).**
- **Use a password that includes some nonalphabetic characters, such as digits or punctuation marks.**
- **Use a password that is easy to remember, because you don't want to write it down. Use a password you can type quickly without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder. Be wary of typing passwords in front of others.**
- **Change your password on a regular basis. Try to change it every three months.**

Ref: Cisco.Press.Designing.Network.Security_ebook

Infrastructure and Data Integrity

- On the network infrastructure, you want to ensure as best you can that any traffic on the network is valid traffic.
- Valid traffic can be categorized as expected network traffic, such as the following:
  - Supported services
  - Unspoofed traffic
  - Data that has not been altered

Ref: Cisco.Press.Designing.Network.Security_ebook

Firewalls

- A common way to ensure infrastructure integrity is with firewalls.
- A firewall, in its most simplistic sense, controls the flow of traffic.
- Rules are created to permit or deny various types of traffic and parallel any routing decisions made.
- The permission or denial of traffic can include specific network services.
- firewalls are deployed at critical ingress and egress points of the network infrastructure.

  - ** data ingress refers to traffic that comes from outside an organization's network and is transferred into it.
  - ** egress meaning is the process of data leaving a network and transferring to an external location. Data egress is a form of network activity but poses a threat to organizations if it exposes sensitive data to unauthorized or unintended recipients.

Ref: Cisco.Press.Designing.Network.Security_ebook

Firewalls

- **Currently, there are three classifications of firewalls that encompass different filtering characteristics:**
  - **Packet filtering: These firewalls rely solely on the TCP, UDP, ICMP, and IP headers of individual packets to permit or deny traffic. The packet filter looks at a combination of traffic direction (inbound or outbound), IP source and destination address, and TCP or UDP source and destination port numbers.**

    (network layer(layer 3))
  - **Circuit filtering: These firewalls control access by keeping state information and reconstructing the flow of data associated with the traffic. A circuit filter won't pass a packet from one side to the other unless it is part of an established connection.**

    (transport layer (layer 4))
  - **Application gateway: These firewalls process messages specific to particular IP applications. These gateways are tailored to specific protocols and cannot easily protect traffic using newer protocols.**

Ref: Cisco.Press.Designing.Network.Security_ebook

Firewalls

- **Before determining which classifications best fit your environment, examine the traffic flow control you can apply in your environment. Most of the control is based on a combination of the following characteristics:**
  1. **Direction of traffic**
  2. **Traffic origin**
  3. **IP address**
  4. **Port numbers**
  5. **Authentication**
  6. **Application content**

Ref: Cisco.Press.Designing.Network.Security_ebook

Firewalls: traffic flow control

- **Direction of Traffic**
  - **Traffic can be filtered in either the inbound or outbound direction.**
  - **Generally, inbound traffic comes from an outside untrusted source to the inside trusted network.**
  - **Outbound traffic comes from inside the trusted network to an outside untrusted network**

Ref: Cisco.Press.Designing.Network.Security_ebook

Firewalls: traffic flow control

- **Traffic Origin**
  - Whether traffic was initiated from the inside (trusted) network or the outside (untrusted) can be a factor in managing traffic flow.
  - For example, you might want to allow certain UDP packets to originate from inside the trusted network (DNS), but might not allow DNS requests to come in from the outside untrusted network. Alternately, you might want to restrict TCP traffic to outside untrusted networks if the TCP session was initiated from the inside trusted network.
- **IP Address**
  - The source or destination address can be used to filter certain traffic. This approach is useful for implementing precursory controls to help avoid spoofing attacks.
- **Port Numbers**
  - TCP and UDP source and destination port numbers are used to recognize and filter different types of services.

Ref: Cisco.Press.Designing.Network.Security_ebook

Firewalls: traffic flow control

- **Authentication**
  - At some ingress points to trusted networks, you might want to authenticate users before they can access particular services, such as Telnet, FTP, or HTTP.
  - Available authentication mechanisms vary, but they all aid in controlling use and auditing who is accessing which services. As an aside, authentication can also help service providers with billing and accounting information.
- **Application Content**
  - It can be useful to look at applications and determine certain controls. You might want to look into filtering certain Uniform Resource Locators (URLs) or filtering specific content types (such as Java applets).

Ref: Cisco.Press.Designing.Network.Security_ebook

Network Services

- **Choosing which services and protocols you support can be a daunting task.**
- **An easy approach is to permit all and deny as needed.**
  - **This policy is easy to implement because all you have to do is turn on all services and allow all protocols to travel across network boundaries. As security holes become apparent, you restrict or patch those services at either the host or network level. This approach is fairly simple, but it is also vulnerable to a multitude of attacks.**
- **A more secure approach is to deny all and permit as needed.**
  - **With this method, you turn off all services and selectively enable services on a case-by-case basis as they are needed. The deny-all model is generally more secure than the permit-all model, but it requires more work to successfully implement. It also requires a better understanding of the services.**
- **If you allow only known services, you provide for a better analysis of a particular service or protocol and you can design a security mechanism suited to the security level of the site.**

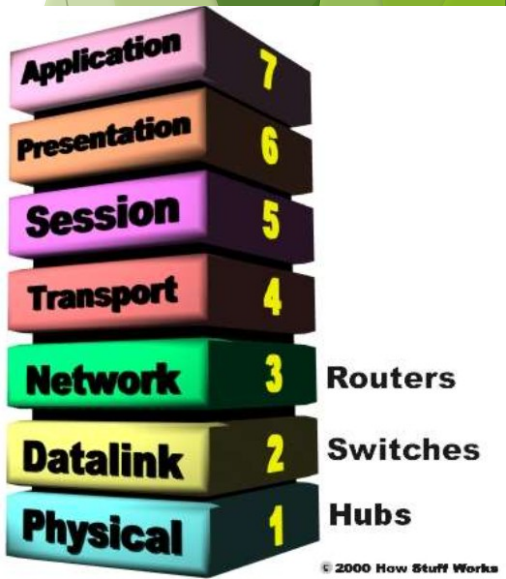
Ref: Cisco.Press.Designing.Network.Security_ebook

Securing the Switch

Switch Security Best Practices

- Once you have configured your switches according to the basic set up instructions above, it's time to think about security.
- Set Passwords and Usernames for Console and CLI Access – Configure strong, unique passwords for CLI Access method and levels of authorization. While usernames aren't required, it's a good opportunity to set them up as well to avoid any complications with third-party management tools that may have issue with blank username fields.
- Secure SNMP with Custom Strings – Communications sent via SNMP are not encrypted and can be intercepted or sniffed unless you set up custom strings. Also, disable any default strings. Update your network management tools once you've changed the strings.
- Enable SSH and Disable Telnet – SSH encrypts communications between the terminal and the switch to prevent man-in-the-middle attacks. Create a public/private SSH key for each switch. Test to make sure it's working and then disable Telnet.
- Enable HTTPS and Disable HTTP – Create a certificate that the switch will use to authenticate with the browser. HTTPS ensures that management traffic, including login and other sensitive information on the web, will be encrypted.
- You can use this post as a checklist when configuring and installing switches on your network or consider adding this information to your documentation. By following these best practices and security tips, you're setting up your network to be stable and secure, as well as easy to troubleshoot when things do go wrong.

Ref: https://www.summit360.com/2019/01/11/switch-configuration-and-security/



- **Switch port security limits the number of valid MAC addresses allowed on a port.**
- **When a MAC address or a group of MAC addresses are configured to enable switch port security, the switch will forward packets only to the devices using those MAC addresses.**
- **Any packet from another device is discarded by the switch as soon as it arrives on the switch port.**

Ref: https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-switching/cisco-ccna-port-security-and-configuration/

Securing the Switch

- **How to Secure Switch from unauthorized access**
- **https://www.youtube.com/watch?v=dXsVAabXU0E**
- **Please watch this video.**

Securing the Router

- **Wireless internet or Wi-Fi access has become a necessity in the home and workplace, but it can also open a door to risks from hackers, scammers, and identity thieves. Whether in your home or office, an unsecured Wi-Fi router running on the default manufacturer settings could be a liability when it comes to hackers and Wi-Fi squatters accessing your private information and burdening your broadband.**
- **If your Wi-Fi network isn't secured properly — a public IP address, no unique Wi-Fi password — you could be letting anyone with a wireless-enabled device gain access.**
- **You might not be worried about someone using your wireless connection, but the real risk is exposing sensitive information you send and receive — your emails, banking information, and maybe even your smart home's daily schedule — to cybercriminals.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

Wireless router

- **Basic router security**
- **Every router should have a strong password .**
- **Some new routers come with default passwords, but you should change these during setup.**
- **Specific instructions vary from one router to another, but the basic idea is this:**
  1. **All wireless routers have a numerical address. If you've lost the instructions, you can probably find yours by searching online for your router's model number.**
  2. **In Security Settings, create a name for the router, and a password, and then select a type of encryption.**
  3. **Make sure you choose a complex password that you can remember, but one that's not easy to guess.**
  4. **Don't forget to save the updated information when prompted. Your router is now secured against roaming cybercriminals.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-

- **Different types of encryption**
- **Depending on your router, you might have options for different kinds of encryption. The most common router encryption types are WEP, WPA, and WPA2. Commercial routers from brands like Netgear, Linksys, and ASUS often include:**
  - **Wired Equivalent Privacy (WEP): This is the oldest and most popular form of router encryption available. However, it is the least secure of all encryption protocols. It uses radio waves that are easy to crack. Every data packet that is transmitted uses the same encryption key. With the help of automated software, this information can easily be analyzed.**
  - **Wi-Fi Protected Access (WPA): The Wi-Fi Alliance came up with WPA to offer an encryption protocol without the shortcomings of WEP. It scrambles the encryption key thereby getting rid of the problems caused by hackers cracking the radio waves. This is also a less secure form of encryption, partly because of legacy hardware and firmware that still used WEP as their main protocol. However, it is a significant improvement over WEP.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-

- **Wi-Fi Protected Access 2 (WPA2): This encryption type is currently the most secure and most recent form of encryption available. You should always select WPA2 if it is available. It not only scrambles the encryption key but it also does not allow the use of Temporal Key Integrity Protocol or TKIP which is known to be less secure than AES.**
- **Advanced Encryption Standard: When possible, you'll want to use AES on top of WPA2 or WPA. This is the same type of encryption used by the federal government to secure classified information. Routers made after 2006 should have the option to enable this on top of WPA2.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-

How to set up Wi-Fi router securely: The specifics

- **Update your router with new firmware and keep it up to date**
  - **Updating your router's firmware is an important security measure to help protect your router against the latest threats. Most modern routers allow you to enable notifications to prompt you when the manufacturer makes patches and updates to the router's firmware available.**
- **Change your login credentials and router password**
  - **Traditional routers come with a default password created by the manufacturer.**
  - **Make sure you change the password of your router during setup. Choose a complex alphanumerical password with multiple characters. If possible, change the username of your network, too. After all, it makes up half of the log-in credentials.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

- **Always use WPA2 to secure your wireless network**
  - **Wi-Fi Protected Access 2, better known as WPA2, is a commonly used network security technology used on wireless routers.**
  - **It is one of the most secure encryption options available in the market since 2006. WPA2 scrambles the traffic going in and out of the router. That means even if someone is within range and can see traffic, all they see is the encrypted version.**
- **Disable WPS, Remote Access, and UPnP**
  - **Wi-Fi Protected Setup (WPS) was created with the intention of making the user experience easier and quicker when connecting new devices to the network. It works on the idea that you press a button on the router and a button on the device. This makes both devices pair automatically.**
  - **Remote Access-A lot of routers come with features designed to make remote access from outside your home easier, but unless you need admin-level access to your router from somewhere else, you can usually safely turn these features off from the router settings panel. Besides, most remote access apps work fine without them.**
  - **UPnP-Universal Plug and Play. Designed to make it easier for devices like game consoles and smart TVs to access the web without making you wade through a lot of configuration screens; UPnP can also be used by malware programs to get high-level access to your router's security settings.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

- **Get rid of any risky or unverified services**
  - **It would be wise to disable remote access to your router when you are actively connected to it.**
  - **Take UPnP, for example. Universal Plug and Play or UPnP is an easy way to allow devices to find other devices on your network. It can also alter the router to allow devices from other networks to access your device. However, it has helped hackers to introduce malware and viruses by making them bypass the firewall.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

- **Setup a guest network for smart home devices**
  - **A guest network has its advantages. It not only provides your guests with a unique SSID and password, but it also restricts outsiders from accessing your primary network where your connected devices work.**
  - **hide the SSID of your main network—basically the name of the network that appears when your devices scan for Wi-Fi.**
- **Use a virtual private network or VPN**
  - **A virtual private network (VPN) encrypts connections between devices, creating online privacy and anonymity.**
  - **A VPN can mask your internet protocol (IP) address so your online actions are virtually untraceable. VPN services establish secure and encrypted connections to provide greater privacy of the data you send and receive, even on secured Wi-Fi hotspots.**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-

- **Always use a firewall**
  - **A firewall monitors incoming and outgoing network traffic and allows or blocks specific traffic. It is an important security feature to look for when selecting a router. For the online safety of your network and devices, it's smart to never disable a firewall.**
  - **Install and use a strong antivirus and security software**

Ref: https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

The End

TASBIH KIFARAH

Ucapan doa pada akhir majlis:

سُبْحَانَكَ اللَّهُمَّ وَبِحَمْدِكَ

اَشْهَدُ اَنْ لاَ اِلَهَ اِلاَّ اَنْتَ

اَسْتَغْفِرُكَ وَاَتُوْبُ اِلَيْكَ

Maha Suci Engkau, ya Allah, dan dengan memuji Mu,
aku bersaksi bahawa tiada Tuhan yang berhak disembah melainkan Engkau,
aku meminta ampun dan bertaubat kepada Mu