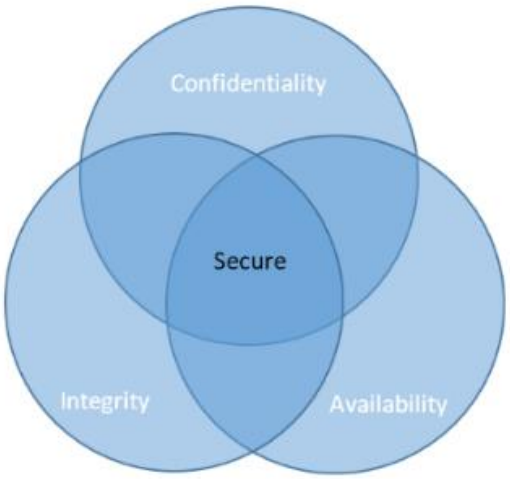
WHAT IF SOMEONE IS SPYING ON YOU

While you are on internet, what if someone stealing your data? What if someone is capturing your data packets? There are many ways a hacker can enter in your network and gain your data and information and use your information the way they want to.

CIA - Confidentiality, Integrity and Availability

Most Important factors to be secure CIA i.e. Confidentiality, Integrity and Availability
Confidentiality means keeping sensitive information private. This involves ensuring that only who have authority to access and preventing that are not authorized.
Integrity means ensuring the quality. This ensures that data has not been tempered and can be trusted. Integrity includes hashing, digital signature, audition and version control.
Availability means that system, network and applications are running. It ensures that application is available for users who all have authority.



SOME NEWS

It's very important to make sure that you are using a safe internet connection. You should be vulnerable free to stay safe. Recently 100 GB data of Indians sold on dark web. This includes passports, PAN cards, Aadhar Card, Voter IDs and driver license
On 21- Apr-2020, 267 Million Accounts sold on Dark Web and hackers leaked employee credential on dark web.

Types of Network Attacks

There are number of attacks an attacker can perform to harm you and your system. Few of them are:-

- DNS Cache Poisoning Attack – A attack that tricks DNS of a system to perform according to attacker
- Man-in-the Middle attack – This is an attack where attacker secretly alters the communication between source and destination. This is done by Session Hijacking, Cookies Hijacking or performing Evil-Twin.
- DOS (Denial-of-Service) – Attack performed to make the system unusable. This is possible by performing Ping of Death(POD), SYN Flood, Half-Open Attack and Distributed Denial Of Service(DDOS)
- Client-side Attack – This attack occurs when user download some malicious data. When user download something but in back something malicious is also downloading in the back without knowledge of user.
- Password Attack – Attack on passwords of the user. This is possible by Brute Force Attack and Password attack.
- Social Engineering Attack – Attack done by social engineering like by fraud calls.

When we are using internet connection, we are connected with large number of hardware and software and vulnerability could be finding in any of this which becomes gold mine for Hackers. We should make sure that our network is secure in every aspect and there are many ways to be secure on Internet:

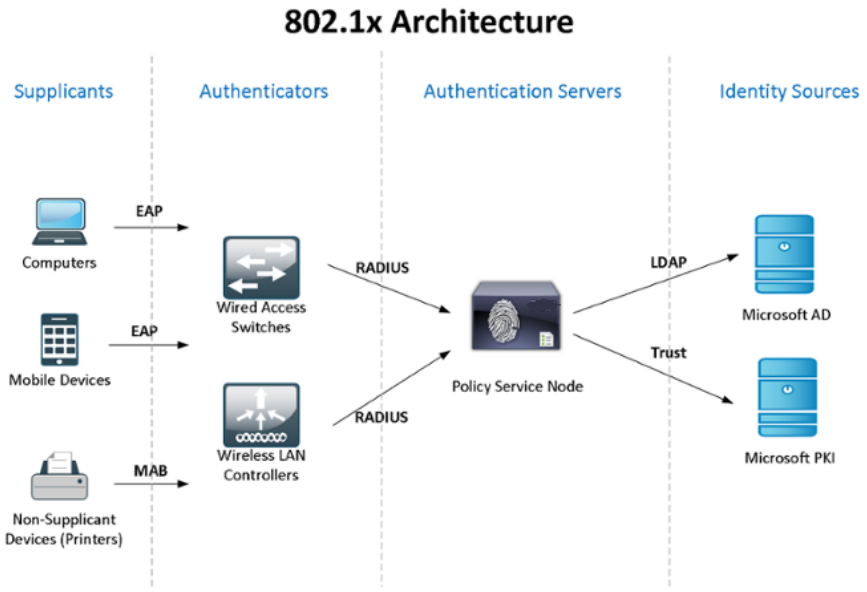
- Network Hardening
- Network Hardware Hardening
- Network software Hardening
- wireless Network security
- Network monitoring

Network Hardening

A way to securing your network by decreasing vulnerabilities which could be done by disabling unnecessary services running. We can use a concept of Implicit deny where anything not allowed should be denied. This can be done by ACL configurations usually configured on firewall where firewall rules are written. Instead of listing what not allowed called blacklisting, you can just list what all allowed called whitelisting. Whitelisting is much easier than blacklisting.

Network Hardware Hardening

1. DHCP is a target for attacker because it is an important protocol in our network. They will get many information like gateway address which can give access to them and also will open door for further attack. so to protect against DHCP attack we use switch which offer DHCP Snooping which will track your DHCP traffic and IP assignments.
2. Another method is Dynamic ARP inspection. ARP has unauthenticated nature which can allow for man-in-middle attack and allow attacker to forge an ARP response. Dynamic ARP inspection will detect the forged ARP packet and drop them.
3. IP Source Guard and IPSG can be enabled to prevent from IP spoofing attack.
4. Implement 802.1X for encapsulating EAP traffic over 802 networks.

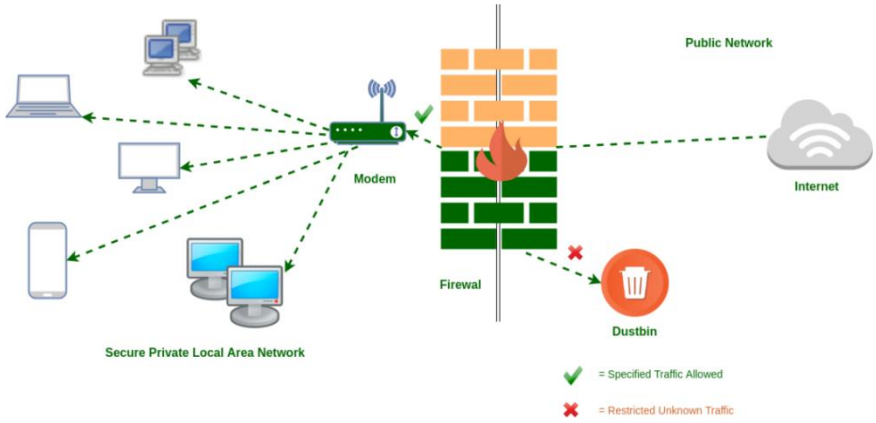


Purpose of 802.1X is to allow or not the users who want full access to network. It is software on client device that make sure of authentication.

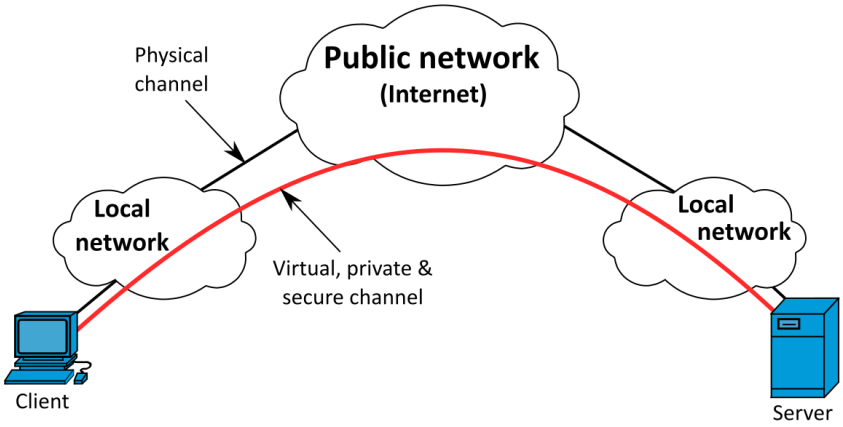
Network Software Hardening

This is important as it plays an important role in securing network and their traffic

1. **Firewall:** There are 2 types of firewalls Host-Based Firewall and Network-Based Firewall. Host-Based firewall protects mobile-phone and laptops that could be used in untrusted or malicious environment like public Wi-Fi. Network-based firewall is built-in firewall in Cisco devices like your router at home has built in firewall and one more example is Amazon firewall in AWS environment.

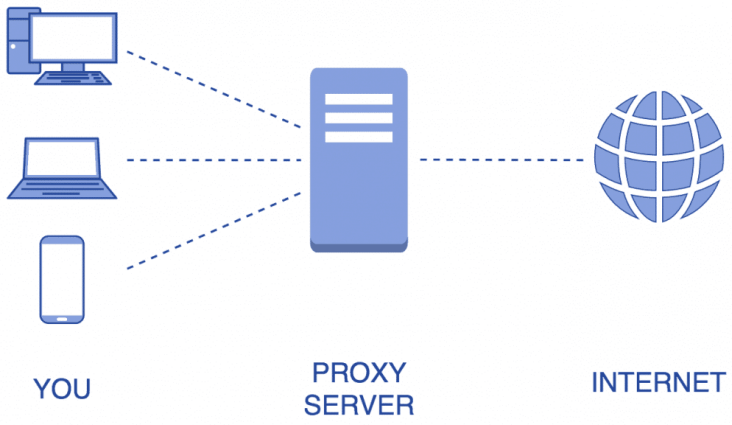


2. **VPN:** Virtual private network uses a tunneling process from one to another. Data transferring between them is encrypted which is decrypted at the end.



It creates a point-to-point connection between client and server by tunneling over the existing network. VPN provides confidentiality such if packet is sniffed the hacker will get encrypted data. It also provides message integrity to detect any instance of tempering with ongoing messages.

3. **Proxy:** Using proxy reduces the chance of getting attack. Proxy is a gateway between you and internet. When attacker will try to attack they will have proxy IP and you will be less vulnerable.

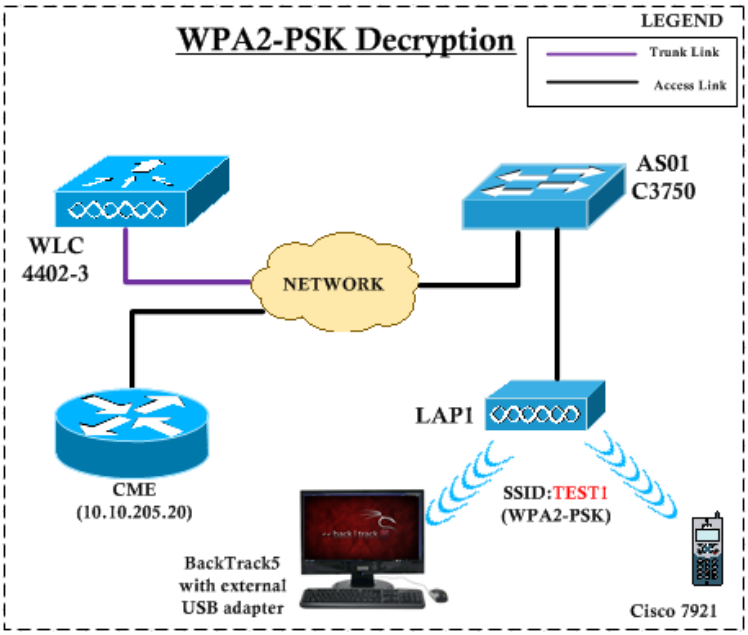


Proxy acts as a gateway between user and internet which makes you secure. When someone try to reach you they will be able to reach to your proxy who will pretend to be you. If they get the IP, they will get the IP of proxy server not yours which makes you anonymous.

Wireless Network Security

Wireless Network like Wi-Fi is also necessary to be secure.

1. 802.1X - we can protect Wireless Network by using 802.1X with EAP-TLS. This is a complex method.
2. WEP - Wired Equivalent Privacy Protocol is a weak security method. It encrypts with 256-bit key and can be cracked easily so there are alternatives to use.
3. WPA or WPA2- Wi-Fi protected Access security protocol. Here long random password or passphrase makes uncrackable. It uses TKIP encryption algorithm which makes more secure.
4. WPA2 with AES/CCMP Mode- we can use this to protect from brute force attack as longer the passphrase increase the amount to break.
5. Changing SSID - changing SSID to unique will make rainbow tables attack less likely.



Network Monitoring

A method to check where your data packets are going and from where or through which port packets are coming. Many tools are used to capture and analyze the packets from network traffic also called packet sniffing. Like Air crack-ng and Kismet. They capture details like source address, source port, destination address, and destination port, TCP flags and TCP sequence number, ACK number, TCP window size and TCP options, if there are any set.

- Tcpdump - command-line utility used to capture and analyze the packet. It also writes the captured packet details in file for further analyzing.
- Wireshark- another packet capture and analysis tool that you can use, but its way more powerful packet analysis. It's a graphical utility which makes easy to analyze.