Lecturecast 3: Network Tools and Components

LAN: Local Area Networks is the most common form of home network and can be implemented in various ways. The star topology became widely accepted as it allows devices to connect to a common **hub/switch** thereby making it easier to expand the network and limiting faults to a specific equipment.

Some Security risks applicable to **Enterprise switches** are eavesdropping and port mirroring

Wi-Fi was established in 1999. A radio-based communication link running at either 2.5GHz or 5GHz. It uses CSMA/CA as its MAC address. Because it uses radio as a means of communication, data could be intercepted and this is why data across a wi-fi network should be encrypted. Common encryption techniques are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). WPA was developed to mitigate some of the security issues with WEP such as possibility of cracking a WEP key (Aircrack-ng is a tool that can be used for this). WPA 2 uses advanced encryption mechanism AES cipher but has also recently been compromised

Modem: used to connect a LAN to a WAN. There are various types of modem offering different speeds

WAN (Wide Area Network): is the backbone technology of the internet. It uses **routers** which directs packets to various location based on data in a routing table. Security risks applicable to the use of routers are Route poisoning, overfilling of routing tables and routers not updated with unavailable routes.

Wireless communication on WANs are done via cellular technology however cellular modems are subject to security issues and concerns:

- They should be regularly patched and updated as they are software-based devices
- Third party applications should be checked for security threats

Major risks are confidential data leakage, denial of service type attacks, jailbreaking etc. GSM devices use A5 encryption. 3G devices use A5/3 and A5/4.

Firewall

Most popular security device/application in use today. It Could be a physical, virtual appliance or software application. Used for packet filtering but overtime, firewalls were not sufficient in preventing attacks.

Host machines had anti-virus scanners, intrusion detection and prevention systems, spam filters, URL & content filtering applications. Combination of these devices are known as UTM (Unified threat Management) and they form third generation Firewall application.

It is important to ensure a firewall's software is regularly patched and maintained and its security certificates and passwords are regularly maintained.

NOS Network Operating System

Operating systems also have their own security risks.

Cloud computing

Cloud computing is beneficial to business and individuals. It is the most common example of virtualisation and is available in many configurations. IaaS, PaaS and SaaS

Security concerns with cloud technology include data storage falling foul of GDPR guidelines , inadequate separation of multiple clients resources and API security

Packet Diagnostic and Analytic tools

TCPDump

Wireshark: This is preferred because of ease of use. It is GUI based.

Vulnerability and Port Scanners

Nmap, Nessus, OpenVAS, Kali Linux