Security issues that are considered when implementing a wireless lan course work

Law, Security

Wireless LAN has various advantages including cost advantage, convenience and productivity. However, the radio waves subject the network to various risks which can lead to hacking. The three main security issues considered before implementing a Wireless LAN are highlighted hereunder.

Denial of Service

Here, the network intruder floods messages, either valid or invalid, into the network. These messages affect the availability of the resources of the network. WLAN are highly vulnerable against this kind of attack. WLAN has relatively low bit rates which can easily get overwhelmed, exposing them to denial of service attacks. During the implementation of a WLAN, powerful transceiver should be used.

Spoofing and Session Hijacking

Here, the attacker assumes the identity of a valid user and is able to gain access to the resources and the privileged data in the network. This is possible since the 802. 11 networks don’t authenticate the address of the source (Medium Access Control Address). The MAC addresses can therefore be spoofed and the sessions hijacked by the attackers. To curb this, proper authentication and access control measures should be put in place during the implementation of the WLAN.

Eavesdropping

Here, the confidentiality of the transmitted data across the network is attacked. It is always impossible to control the recipients of the signals in any WLAN system since the WLANs radiate network traffic into space

intentionally. Eavesdropping is therefore possible by any third party, making it the most significant threat in a WLAN. The transmission can be intercepted by the attackers at some distance.

Network Topologies

Bus Topology

In a bus network, a common backbone is used to connect all the devices. The single cable (backbone) acts as a shared medium of communication and devices are attached to it via interface connectors.

Its main advantage is that, it is easy to install and does not need much cabling as compared to other topologies. However, the network cannot work with several devices as this result in performance problems. The number of devices must be limited. Also, any failure in the backbone cable renders the entire network unusable.

Ring Topology

In this network, every device is connected to two neighboring devices, and data travels in one way. It’s easy to implement; however, adding another device can be tricky. Any failure in the device or cable can break down the entire network. A failure in any cable or device breaks the loop and can break down the entire network.

Star Topology

In a star connection, there is the central connection point (hub). The central connection point may be a hub, router, or switch. All other devices are connected to the hub via Unshielded Twisted Pair (UTP) Ethernet. Its main

advantage is that, a failure in any cable or device does not affect the network. The entire network only fails as a result of a failure of the hub. This topology uses more cables.

Mesh Topology

In this topology, every device is connected to each other device within the network via its own cable. The disadvantage is that, in any sizable network, large amounts of cables are used. This topology is the most expensive. Its main advantage is its high fault tolerance.

Ethernet, Token Ring, FIDDI and wireless

Ethernet is a family of networking technologies for LANs. It’s standardized as IEEE 802. 3. It employs the use of CSMA/CD (Carrier Sense Multiple Access with Collision Detection). FDDI (Fiber Distributed Data Interface) is used to provide a standard for the transmission of data in a LAN that extends in a range of up to 124 miles. Its main advantage is the large geographic coverage area. FDDI LANs can also support unlimited users. Token ring LAN has a deterministic access method which gives it a better performance and greater reliability for very critical applications as compared to Ethernet. Its main disadvantage is the Micro Channel architecture. Wireless does not use the hard wired connection. It is the information transfer over some distance, without the use of wires. The distance is relative.

Levels of the OSI model where TCP/IP functions

Of the seven layers of the OSI, only four are adopted for TCP/IP architecture. This architecture combines some features of the adjacent layers of OSI and

at the same time omits some features. The four levels are the application layer, the transport layer, the network layer, and the network access layer.

Reference

Bicsi, B., (2002). Network Design Basics for Cabling Professionals. City: McGraw-Hill Professional

Bush, R. and Meyer, D. (2002). “ Some Internet Architectural Guidelines and Philosophy”, Internet Engineering Task Force. Retrieved at http://www. isi. edu/in-notes/rfc3439. txt

Hamid, R. A. (2003). Wireless LAN: Security Issues and Solutions. SANS Institute. Retrieved at http://www. sans. org/reading_room/whitepapers/wireless/wireless-lan-security-issues-solutions_1009

Inc, S., (2002). Networking Complete. Third Edition. San Francisco: Sybex

Mark, D. et al. (2007). Network Fundamentals: CCNA Exploration Companion Guide.