Wireless network

Business

The Wired Equivalent Privacy protects data, as it moves via the airwaves in a wireless network. After the release of the Wired Equivalent Privacy encryption, security issues arose about the vulnerability of its connections. Attacks on wireless network begin with knowledge of the location of the network.

This commences by determination of its station and its subsequent access point. Upon determination of the two, the intruder footprints the wireless network actively or passively. The active method involves the use of a station to acquire a Service Set Identification. In the passive method, the intruder monitors the airwaves and detects live access points, service set identifications and stations. Trace method of intrusion shows extends, at which the wireless network is vulnerable.

An intruder monitors the network and identifies a beacon, sent out by an access point. This enables the station to know the existence of a live access point. This packet might contain the Service Set Identification details that the intruder uses to access further details that lead him to access secured servers. The Wired Equivalent Privacy algorithm is still vulnerable to Brute Force Attack (Schneier, 1996). The algorithm uses a symmetric cryptography system that allows users to use shared codes and passwords.

Vulnerability arises from the little information, an intruder needs to determine passwords. This is because of the small space in he pseudo random number generator, used to encrypt such passwords. There also arises a weakness in the random key generator of the Wired Equivalent Algorithm. This enables intruders to collect enough packets that help them identify user passwords and codes. The inability of the Wired Equivalent Privacy to protect encrypted data from damage on alterations causes its vulnerability to bit-manipulation attack.

The cryptography system of a wireless network performs bit-by-bit operations, thus, makes intruders able to disrupt access by changing a single bit. This single change denies the access to information. Firewall Firewalls have a design that protects computers that have networks from unauthorized access. Firewalls come in the form of software or hardware devices. A firewall majorly contains an interface for the network that it protects and an interface for the network that the computer exposes it to, while working. The firewall, therefore, performs its functions at the junction of the two networks, accessed by the computer (Chapman, 1995).

Firewall does not protect all the data, available in a network. Protection of wireless networks involves procedures that protect the aspect of integrity, confidentiality, and authentication. Although firewall provides all these services, it only does so to the information and data behind it. Other information, not within firewalls transit, is vulnerable to attack by hackers. This makes it easy for intruders to access data, not behind firewalls transit in a firewall-protected system.

Apart from failing to solve all the problems, firewall has its own problems that increase insecurity. It restricts access to information that would otherwise be of use in securing data. It also focuses its security on a single area, thus, leading to insecurity or limited access to the network, which is a disadvantage to users. MeasuresPractice of common activities such as changing Service Set Identification helps to secure wireless networks. Since a potential hacker accesses SSID with ease, forming a unique SSID is vital.

Use of SSID that do not have company initials prevents attacks. Users ought to configure their access points well and change default passwords, SSID, and Simple Network Management Protocols. Use of other privacy along with the WEP helps in reducing vulnerability of networks (Kaufman, 1995). Use of certificates to authenticate and authorize access is safe. This reduces the changes of an intruder, accessing private information. Segments in wireless internet serve as a precaution in case of an attack.

A filter placed between the access point and the internet lowers the level of damage in case an intruder acquires an Access Point. Physical protections are also vital. This comprises of use of antennas and shielding premises from the entrance of electromagnetic waves (Kaufman, 1995).