

Wireless Network Security – Are you secure?

Overview

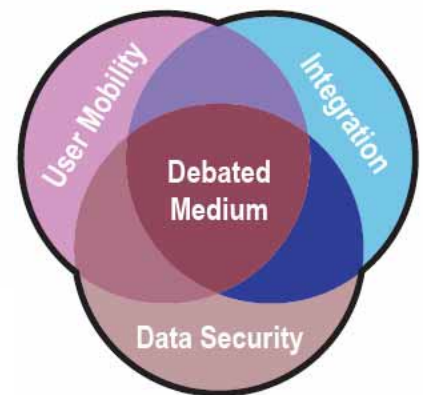
Wireless security has become a hot topic in recent years with businesses blindly adopting this new form on network communication with hopes of increased user mobility and convenience. Would you ever stand on the corner of a busy intersection in downtown Chicago with your wallet open, credit cards dangling in a plastic holder open for every passing car to gaze at and take home to use? No. We keep our wallets closed, account numbers private and records of transactions between the bank and the customer.

Threefold Conflict

There are many factors that come into play when thinking about developing and deploying a wireless solution for your organization. The first topic that comes into play when deploying a wireless network is freedom from a physical, or 'wired' network; the connection between the end servers and other network devices is now dynamic and the end user can wander around the office and receive data from differing locations. This is the main benefit in the deployment of a wireless network; however, there are two other factors that must be considered before adopting the new network topology.

The topic of data security is in conflict with increased user mobility. The user is no longer bound to be physically in the reach of the network wiring. The wireless signal propagates in an omni-directional sphere in free space and, therefore, may penetrate the floor and be able to be picked up outside the physical boundaries of the parent office; this can be a major breach in security.

The third concern when deploying a wireless network is integration. This is something which must be considered in conjunction with the other two concerns of data security and user mobility. Increasing the data security may mean adding new network protocols or new authentication procedures which will, in turn, diminish the area of user mobility. The debated medium may mean sacrifices in user mobility to increase data security and integrating with the existing network may mean a loss in data security. The three factors are in conflict with each other, where an increase in one means a reduction in one or both of the other factors.



Additional Considerations

Unlike wired media such as Coax cable, Ethernet cable or even fiber based communications, the signal in a wireless environment is not confined to one physical wire. The radio signal may pass through a wall, across the street and be able to be received in a neighboring office. Depending on the type of obstacles that the wireless signal has to penetrate, it could propagate anywhere from 10 to 200 feet, or in some cases even farther.

Insecure Networks

There are a few characteristics that classify a wireless access point as insecure. Generally, we can define an insecure access point as being open to a foreign connection and allowing the foreign connection to pass data to or from the host network. Some of the major security holes that are often left unchanged from a default configuration are:

Apogee Strategies LLC

Chicago Downtown Office

6 West Hubbard St., Suite 300 Chicago, IL 60610

Chicago Suburban Office

1300 Higgins Rd., Suite 301 Park Ridge, IL 60068

Toll free 877/871-8211 Fax 312/327-2221

www.apogeestrategies.com





Innovating the Technology of

Information

Conclusion

The deployment of a wireless network comes with many benefits in terms of mobility, usability and flexibility. However, there are many security factors to consider before beginning any deployment. Encryption, location of the access point and initial setup can all determine if your network will be easily targeted by intruders or eavesdroppers. The degree to which a network needs to be secured can only be determined by carefully evaluating the risks. For example, considering what geographic locations can receive your signal may dictate your level of caution. If your signal can only be received by two adjacent offices, your chances of a major hacking attempt is less than if your signal is accessible from a public space or another building. Only a seasoned I/T professional with experience in network security and wireless technologies can adequately configure and protect your data and resources from intruders.

For more information about network security, wireless networks or other networking/security concerns, contact Apogee Strategies LLC for a consultation.

Apogee Strategies LLC

Chicago Downtown Office

6 West Hubbard St., Suite 300 Chicago, IL 60610

Chicago Suburban Office

1300 Higgins Rd., Suite 301 Park Ridge, IL 60068
Toll free 877/871-8211 Fax 312/327-2221

www.apogeestrategies.com

