Wireless security essay

Business, Industries

The advent of Information and Communications Technology has brought a lot of changes in today's modern world. Many technologies are available in the market today that brings improvement in almost all aspects of development. One of these technologies is the establishment of a network.

A network is, basically, consists of computers or node connected together to share resources. One network can interconnect another network either through wired or wireless communication paths. A network should have these four things – HUB to perform traffic control, CABLE which is used to connect all medium, Network Interface Card (NIC) which is plugged into the computer to be able to send and receive messages and PROTOCOL which is the language used to communicate among nodes in the network (Jelen, 2003). In a network, processes may institute a session to exchange information.

There are different ways to connect processes to communicate over the network. One common scheme is circuit switching which establishes a permanent physical link between computers. This link is allocated for the entire duration of the communication. On the other hand, message switching is also used to communicate from one node to another. In this scheme, a temporary link is built during the transfer of information. Another scheme used is packet switching which divides the message into a number of packets and each packet is sent to its destination separately.

(Silberschatz & Galvin. , 1998 p489) Introduction Where there are people, there will be technology, because the world needs it to survive. In the present, technology is all around us. Every where you go you run into some type of technology, whether you know it or not. Advancement in technology makes everyday things easier than they have ever been before. But as an evolving society, new technologies are what drive the world today: 3G mobile communications, Voice over Internet Protocol, Bluetooth, and wireless devices are the new driving forces, but where will they take us? Wireless devices, like all technologies that provide external access to corporate networks, present security challenges. With wireless standards and practices still rapidly evolving, it is important to understand the strengths and limitations of available technologies in order to implement a secure solution.

Extending current security policies to encompass wireless devices requires an understanding of the security features of both wireless devices and wireless networks. Types of Wireless Networks The Wireless Market Over the past ten years or so an alternative to wired LAN structures has evolved in the form of the Wireless LAN. The first generation Wireless LAN products, operating in unlicensed 900-928 MHz Industrial Scientific and Medical (ISM) band, with low range and throughput offering (500 Kbps), subjected to interference came to market with few successes in some applications. But they enjoyed reputation of being inexpensive due to break through development in semiconductor technologies, on the other hand the band become crowded with other products with in short period of time leaving no room for further development. The second generation in 2. 40-2. 83 GHz ISM band WLAN products boosted by the development of semiconductor technology was developed by a huge number of manufactures.

Using Spread spectrum technology and modern modulation schemes this generation products were able to provide data rate up to 2 Mbps, but again the band become crowded since [the] most widely used product in 2. 4 GHz is [the] microwave oven which caused interference. Third generation product[s] assembled with more complex modulation in [the] 2.

4 GHz band allows 11 Mbps data rate. In June 1997, the IEEE finalized the initial standard for wireless LANs: IEEE 802. 1. [The] [f]irst fourth generation standard, HiperLAN, came as specification from European Telecommunication Standard Institute (ETSI) Broadband Radio Access Network (BRAN) in 1996 operating at 5 GHz band. Unlike the lower frequency bands used in prior generations of WLAN products, the 5 GHz bands do not have a large “ indigenous population” of potential [interferers] like microwave ovens or industrial heating system as was true in 900 MHz and 2. 4 GHz [8]. In late 1999, IEEE published two supplements to the 802.

11: 802. 11b and 802. 1a following the predecessor success and interest from the industry. ETSIs next generation HiperLAN family, HiperLAN/2, proposed in 1999 operating at same band with its predecessor, is still under development, the goal is to provide high-speed (raw bit rate 54Mbps) communications access to different broadband core networks and moving terminals.

It is expected that 802. 11b will compete with HiperLAN/1 and 802. 11a will compete with HiperLAN/2 in near future. [5] As wireless technology matures, newer features and functionality will continue to be made available. Standardization organizations, like IEEE, ETSI, are providing continuous effort to meet new demands from user by introducing new standards as well as minimizing shortcomings of the previous standards. This includes performance fine-tuning, like smother and seamless roaming capabilities as well as QoS and most importantly security features.

These standards are currently in development, and will sit atop of existing ones delivering more robust performance Wireless LAN. [5] The wireless market is expected to grow significantly over the next several years. As this growth occurs, solution providers will also be expected to address security concerns. [6] Wireless LAN is experiencing tremendous change in today's modern world since there is an increase in bandwidth provided by IEEE 802. 11 standard.

The table below shows the characteristics of WLAN technology. Table 1: Key Characteristics of WLAN Characteristics Description Physical Layer Direct Sequence Spread Spectrum (DSSS), Frequency Hoping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), Infrared (IR) Frequency Band 2. 4 GHz (ISM band) and 5 GHz. Data Rates 1 Mbps, 2 Mbps, 5. 5 Mbps, 11 Mbps, 54 Mbps Data and Network Security RC4-based stream encryption algorithm for confidentiality, authentication and integrity. Limited Key management. Operating Range Up to 150 feet indoors and 1500 feet outdoors Positive Aspects Ethernet speeds without wires; many different products from many different companies.

Wireless client cards and access point costs are decreasing. Negative Aspects Poor security in Native mode; throughput decrease with distance and load. (Karygiannis & Owens, 2002, p24) Wireless Network Diagram Figure 1: Wireless Network Diagram.

The above figure shows the diagram of a wireless network. This involves the use of wireless router which must possess a working network adapter. A broadband modem which is connected to the wireless router enables the sharing of a high-speed internet connection. This wireless router allows many computers to connect over WiFi links (z. about. com/…

/1/7/g/3/wireless-diagram-1. jpg). Security Threats and Issues The figure below shows the taxonomy of security attacks in WLAN. Figure 2: Taxonomy of Wireless Attacks (Karygiannis & Owens, 2002, p24) Network Security attacks are divided into two attacks – passive and active. Passive attacks happen when an unauthorized party gains full access to the network but do not modify its contents while active attacks occur when an unauthorized party modifies a message, data or a file.

This type of attack may come be masquerading, replay, message modification and denial of service (DoS). Any of these attacks may lead to loss of information, legal and recovery costs, tarnished image and loss of network service (Karygiannis & Owens, 2002, p24). Wireless networks are consisting of multiple stations which communicate through radios and are based on IEEE 802. 11 standards. Aside from the transmission techniques provided by 802. 11, wireless networks have a variety of security mechanisms. The simple protocol defined by 802. 11 is the Wired Equivalent Policy (WEP) which uses a fixed pre-shared key and RC4 cryptographic cipher to encode data transmitted on a network.

All stations connected must agree on the identity of the fixed key to allow exchange of data or information. Another security protocol used is Wi-Fi Protected Access (WPA) which specifies a subset of the requirements found in 802. 11i and defines Temporal Key Integrity Protocol (TKIP) that is derived form the original WEP protocol (Leffler, No Year)Wireless Equivalent Policy (WEP) is specified in the 802. 11b Wireless Standard which is designed to provide a high level of security for Local Area Networks. A wired LAN is protected by physical security mechanisms but this is not effective wireless network because radio waves are not necessarily bound by walls containing the network.

WEP seeks to establish a similar protection for wireless network through data encryption over the network (http://searchsecurity. techtarget. com/sDefinition/0,, sid14_gci549087, 00. html). It is very important for users to secure their networks against all the attacks mentioned in this paper. An important security measure is the usage of a firewall. This means that a few different things offer different security levels.

Using passwords that could be easily remembered is also advisable and it is best to change the password at most every 30 days. In addition, using the username " Administrator" is discouraged since this is automatically created by the system and can be easily tracked by hackers (Bradley, No year) In the aspect of Wide Area Network, wireless communication is gaining its advantage. Wires are no longer needed; telephone jacks are no longer in use and cell phone services are no longer involved. This is advantageous to professionals who work even outside their offices (Oz, 1998 p152). An organization must lay out plans based on the organizational requirements on how to solve network security issues.

The plans should include the needs of the company the needs of the company, policies to support these needs and the amount of physical and logical security needed. A network log should also be in place which describes the actions taken in setting up and supporting network (Tittel & Hudson, p160-161). There are several issues brought by WEP encryption and Shared Key authentication. It is important to note that these are optional; they are turned off in by default in access points. If these are turned on in one of the access points, hackers are given the idea to connect to the network through standard wireless cards and drivers. The signal can travel large distances from the access points and this allows the hackers to connect from outside the building (http://www. research.

ibm. com/gsal/wsa/). Wireless LANs are open to hackers to access relevant information that can spoil the network since these transmit signals through radio waves. Several wireless LANs use spread spectrum which is a modulation technique developed to keep enemy from jamming radio communication and radio-guided missiles.

This is capable of changing the “ spreading codes” in a most secret way. The problem of this is that the 802. 11 publicly describes the spreading codes making it easier for companies to design interoperable 802.

11 components (Geier, 2002). Traditionally, several methods are used to encrypt data streams; all of which uses third-party software to properly

implement it but cannot be easily decrypted when the original data stream is unavailable. The simplest method used is the transition table where each chunk of data is used as an offset in the transition table and the equivalent value is written into the output stream. A modification of this translation table uses two or more tables based on the bytes on the data stream (http://catalog.

com/sft/encrypt. html). On the other hand, Temporal Key Integrity Protocol (TKIP) is another security protocol implemented by the IEEE 802.

11 wireless networks. TKIP uses the same encryption engine and RC4 algorithm as defined in the WEP protocol. This protocol changes the key used for each data packet.

The key is created mixing information of the base key, the MAC address of the transmitting station and the serial number of the packet. This is designed to put a minimum demand on the stations and access points. Each packet has a unique 48-bit serial number incremented every time a new packet is transmitted (http://en.

wikipedia. org/wiki/Temporal_Key_Integrity_Protocol). WiFi Protected Access is one of the first generation of wireless security which provides organizations with a high level of assurance that unauthorized users cannot access the network.

This provides a strong data protection by using data encryption techniques to authenticate users (http://www. wi-fi. org/knowledge_center/wpa). This wireless network setup is easier to use than the wired LAN but there are some serious issues that must be given attention. Appropriate wireless security will eventually overcome these which include unencrypted radio traffic can be hijacked, severe flaws with the radio data encryption algorithm compromise the integrity of data and the lack of scalable user authentication model makes enterprise deployment difficult. Another important aspect of wireless network security is to provide strong authentication and access control at the application layer (http://www. securecomputing.

com/gateway/wireless_network_security. cfm). There have been several ways to impose wireless security issues and it should always start in the access control, providing appropriate access to all users in the network. User authentication is really the most important aspect in networking (http://www. securecomputing. com/gateway/wireless_network_security. cfm).

Conclusion. Wireless technology has become the wave of the future. From cellular phones to wireless point of sale devices, wireless networks and technology is all around us. In order to jump on the wireless train, one must first understand the different standards.

To properly and safely utilize wireless technology the user also must understand the various types of wireless security. Once grasping these technologies and standards, anyone can implement a wireless network in their home. First, the 802. 11b wireless networking standard, which is the most common consumer based standard.

The 802. 11b standards frequency is in the 2. 4 GHz range which is common with most cordless land line telephones and some microwave ovens. There are not really many problems with interference however because you can choose between one of 11 different channels. The speed that is supported by this standard is pretty average at 11mbps but is relatively slow compared to a 100mbps or 1000mbps that is common amongst wired networks. All of this really is not an issue as most consumer broadband internet connections are in the 4-6mbps range anyway. Most wireless hotspots, domestic wireless broadband gateways and company LANs have been using the 802. 11b standard for years now but are slowly moving to stronger and faster wireless networking standards.

The 802. 11a wireless networking standard is not as common as 802. 11b but is still utilized in many wireless networks. Primarily used in Europe and other foreign countries, 802. 11a operates at a higher frequency than 802. 11b at 5 GHz and at a higher speed as well at 55mbps. There are some advantages and disadvantages however to using the 802.

11a wireless networking standard. The first advantage is that it operates at a 5 GHz frequency allowing for less interference as few devices are using this frequency. A disadvantage to this standard is that it has poor performance over longer distances and speed decreases with longer distances as well. An upgrade to 802. 11b is 802. 11g which offers some of the same technology as 802.

11b but with significant upgrades and improvements. The most significant improvement over the 802. 11b standard is the speed. 802. 11g supports speeds upwards of 55mbps which is a huge increase over the 11mbps of 802. 11b. This standard operates at 2.

GHz which is the same frequency that the 802. 11b standard operates at. Another great thing about the 802. 11g technology is it is backwards compatible with a 802. 11b wireless card so there is no need to go out and buy a new wireless network card for your computers.

Finally a brand new standard that is still in its infancy stages and still has yet to be ratified by the IEEE is 802. 11n. 802.

11n will be a huge step towards equality amongst wireless and wired networks. First, the standard sets a speed requirement of at least 100mbps which is common amongst most wired computer networks. It is most likely that the throughput will be in the 200mbps range with a maximum being set in the 600mbps range. Looks like the 802.

11n standard will be operating at both 2. 4 GHz and 5 GHz frequencies. Look for the final 802. 11n draft out in April of 2009.

After choosing a particular standard to go with and buying the equipment to support that standard, one need to know the method of security they wish to implement on their networking equipment to maintain privacy and to prevent others from sharing their internet access. The different types of security come in several varieties such as WEP, WPA, WPA2 and Radius authentication. Each of these different types of security offers a little something different and varying degrees of security. WEP, also known as Wired Equivalency Privacy is the most basic form of security on a wireless network next to no security at all. WEP has encountered tons of scrutiny, many times being referred to as the Weak Encryption Protocol.

After WEP is set up it functions by encrypting the payload of the packet before it is transmitted using RC-4 (Rivest Cipher 4). After the transmission is received it is decrypted by the other station that is also using WEP which virtually means that the security is only in the transmission between the devices. In addition WEP uses only a 40 bit or 64 bit key to encrypt the data. These key lengths are very susceptible to cracking.

Another vulnerability or weakness is that the keys are generally pre-shared and are static which makes it easier to crack because it is non-changing. Another form of security over wireless networks is WPA (WI-FI Protected Access). WPA is far more secure and the most recommended security type used for consumer wireless networks. Instead of using an encryption key, it rather uses a pass phrase between 8 and 63 characters in length. In combination with the SSID, WPA uses TKIP (Temporal Key Integrity Protocol) to generate a unique encryption key for each client. Because the keys are dynamically created there is less concern for cracking.

WPA is infinitely superior to WEP but with any security method in use, nothing is completely secure and hack/crack proof. Although very similar to WPA, WPA2 offers a key upgrade to WPA that offers even more security. One of the biggest improvement was the addition of AES (Advanced Encryption Standard) based algorithm, CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) in addition to TKIP. CCMP is considered fully secure. Finally, one of the most secure methods to wireless security and one used by corporations and other commercial entities worldwide is RADIUS authentication. RADIUS stands for Remote

Authentication Dial in User Service which basically means you must first authenticate with a server separate from the wireless network before even being allowed access to the wireless network. This type of authentication first makes sure you are valid user then passes your information on to the RADIUS server which makes sure that the information is correct using authentication schemes such as PAP Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol) or EAP (Extensible Authentication Protocol).

Many organizations and Internet service providers use RADIUS authentication because various statistics can be logged which can be useful in billing or productivity monitoring. RADIUS although widely used in wireless networks is unfortunately on its way out and will eventually be replaced with DIAMETER which will be quite an upgrade but there may be some compatibility issues. Wireless networking is definitely a great technology and the wave of the future for networking. The biggest thing for consumers to understand that without a little bit of research and education there is the potential for disaster when choosing equipment and implementing the network. With careful research and selection of equipment, consumers can set up a secure and quite effective wireless network. Technology advances so fast and one of the technologies in the world of ICT is wireless networking. Wireless networking provides a very convenient way for professionals and other large-scale enterprises for portability of their documents and work.

This has improved the way business is done today. Indeed, wireless network has brought many changes in today’s modern world. With the birth of this new technology in the networking arena, many threats also arise. To have a smooth exchange of information, security measures are provided so that hackers cannot easily connect to the wireless network.

With the inventions of security measure protocols, it is assured that wireless communication is secured and exchange of sensitive data and information can take place. Wireless security provides all necessary security measures to protect all data and information within the wireless network and to prohibit unauthorized users to have full access to the network. The WEP, WPA and other protocols are used by organizations in implementing security measures.