Implementation of Low Cost Security for WLAN Router Networks (November 2004)

Larix J. Lee, Jason C. Kan, Johnson C. Lee and Michael K. Leung

***Abstract*—This project identifies the security vulnerabilities of Linksys BEFW11S4 Router and explores various methods of increasing security. Solutions explored include VPN – IPsec and PPTP, and physical signal manipulation – signal jamming and signal directing. An implementation of the most cost effective solutions is also discussed in detail.**

***Index Terms*—Linksys Router, Wireless Security, WLAN Security, 802.11b**

I. Introduction

The wireless networking has brought a new era of flexibility and dynamicity into the IT infrastructure for businesses of all shapes and sizes. However, a majority of users of wireless networks are not educated in the security of the wireless networks. Complicating the problem is that many people have the mantra, "If it works, don't fix it", which implies that updating the devices on wireless network or providing a secure infrastructure are not considered priority at all. This project will analyze the 802.11b (wireless-B) network in the context of a small business that is recently made aware of a security issues from a local newspaper, but has limited financial ability to upgrade to the newer devices which support the newer WPA security protocols. A possible network configuration will be determined that will solve the issues outlined by this project. The following example will be used throughout the project as a model for our analysis.

The owner of a small medical-instrument company, MedInstrumentCo, has recently acquired a large office workspace directly upstairs. She currently has her computerized customer database stored in the office downstairs, and would like to shift her networked database and diagnostic computers upstairs, while leaving the Point-of-Sale (POS) equipment downstairs for daily business use. One computer she plans to move upstairs contains highly confidential patient records of people that had volunteered to undergo treatment using the new equipment recently invented by MedInstrumentCo. She bought a LinkSys 802.11b (wireless-B) package from a retail store nearby at discount price, as she knows she has very little left in her funds after acquiring the floor upstairs. She has heard from one of her five employees that there is a newspaper article about someone can listen in on all the network traffic, and would like to investigate this further, as protection of her confidential and proprietary information is of utmost importance to her.

II. Linksys Router Security Weakness

The Linksys Wireless Access Point Router[1] (BEFW11S4) includes security features that improve the wireless network security. In the original package documentation, Linksys states that following a "complete list" of seven recommended steps of protection should give peace of mind while using the router [1]. The seven steps below are taken directly from the Linksys wireless documentation:

> A. Change the default SSID.
> B. Disable SSID Broadcasts.
> C. Change the default password for the Administrator account.
> D. Enable MAC Address Filtering.
> E. Change the SSID periodically.
> F. Enable WEP 128-bit Encryption. Please note that this will reduce your network performance.
> G. Change the WEP encryption keys periodically.

Linksys suggests that steps A through E should be followed for minimal coverage, and provides rationale for each of the five minimal steps. Other security steps that one could take with the router is to disable one of the two antennae, disable DHCP, change IP addressing scheme, and enable logging. Assuming that all the steps outlined above were executed. How secure will the wireless network be? An analysis on each of the suggestions will provide significant insight into this question. The scope of the analysis, will be limited to only the "Infrastructure" configuration, so that all wireless nodes of the network can only communicate to each other via the wireless access point.

Linksys' recommended steps A and B deal with changing and concealing the Service Set Identified (SSID) of the wireless router. The SSID, or the extended version of SSID called the ESSID, is a sequence of alphanumeric characters (up to 32 characters in length) used to identify a wireless network among nodes of the network, and is usually broadcasted by default in a periodically-sent beacon by a router to identify itself [2]. The terms SSID and ESSID are essentially the same and will be used interchangeably. The Linksys router comes pre-configured with the default SSID set as "linksys". Based on a random sample of eight wireless

[1] All subsequence references to Linksys Wireless Access Point Router, (BEFW11S4 version 3.2), will be referred as "Linksys router", "wireless router" or simply "router" unless otherwise stated.

routers targeting small businesses on eBay, typical default SSID's of many different types of wireless access points are the manufacturer's name, model name and number, or simply "default", "ssid" or "wlan". Combined with Linksys' step E, Changing the SSID periodically will prevent unauthorized access to the wireless network simply by guessing or leaving configuration values set to default.

Concealing the SSID is another simple step to deter casual (non-sophisticated) access to the wireless network. This method can be compared to the principal of anonymity, which has a characteristic no one is compelled to answer unless uniquely identified (such as a name). In implementation, the wireless router would leave the SSID field blank in the beacon, or disable the beacon so no one but those who already know the SSID can see the network. However, the SSID can be determined through guesswork (if the default or an deducible SSID is used). Moreover, to a knowledgeable and focused attacker, the SSID can be easily extracted using passive methods (radio frequency monitoring) and determines the SSID from the request of an authorized client requesting a connection [3].

Once the SSID of the wireless router is known, attaching to your network can be trivial if the Dynamic Host Configuration Protocol (DHCP) service is enabled so that an attacker can get a 32-bit Internet Protocol (IP) address for your network. The DHCP server can be provided by the router or by another source in the wireless or wired network connected to the router. In the context of a small business, the list of computers accessing the router is small and will rarely change, so it is unlikely that the dynamic network nature offered by the DHCP service would be used. Therefore, disabling DHCP and assigning static IP's and network configuration to all wired or wireless computers on the network may prevent unauthorized network access. Furthermore, since the Linksys router employs Network Address Translation (NAT) so internal network IP addressing scheme can be different than the external scheme, if the internal scheme is changed from the default "192.168.0.x" scheme to say, "213.321.132.x", then it would be more difficult to guess the network.

Though DHCP is safe for controlled, non-leaking, communication paths like with wired networks, vulnerability exists for open data paths like with wireless, where any one armed with an RF antenna can inject and retrieve data as if he was wired into the network. The Wired Equivalent Privacy protocol attempts to address this issue by providing data encryption such that any wireless communication with the router is hidden from RF eavesdroppers. Unfortunately, the WEP protocol itself has vulnerabilities, resulting in easy deciphering of WEP-encrypted data, and Linksys' steps F and G almost useless. Later enhancements to the WEP algorithm improves upon step G in attempt to correct the vulnerability. Further details on WEP will be discussed later.

With the SSID, IP and data known, an attacker can attempt to change the router configuration for his or her own convenience by attacking the router's administrator account. For example, default router IP addresses are normally configured to be the lowest IP address available in the IP scheme, such as "192.168.0.1" or "213.321.132.1". Relocating the IP of the router to another base address like "192.168.0.199" would also prevent casual attacks. Linksys' step C refers to the case of a more advanced attack made possible as IP's can be simply captured (decryption of WEP), changing the default administrator account and/or password would force the attacker to brute-force the administrator account.

The use of access control lists to prevent unauthorized entities from connecting to the router is a logical and obvious deduction. Media Access Control (MAC) Address filtering, which only allows certain wireless network cards (identified by a unique 48-bit number on each card) to connect to the router. However, MAC addresses can be read from the wireless network traffic, and are not even encrypted when WEP is used. MAC addresses can be spoofed (using manufacturer-supplied drivers for any wireless network card) in seconds using once an authorized MAC address is discovered. Randomly generating MAC addresses to run brute-force attack scripts for each successful connection attempt is possible and often goes undetected in logs [4]. Therefore, Linksys' step D is not effective against more sophisticated attacks, and logging provided by Linksys can only provide a certain level of auditing since the logs do not show the MAC or other lower-abstraction layers.

There are also tools and techniques that assist in detecting the spoofed MAC addresses. Some methods are passive by nature and search for MAC addresses that do not conform to the IEEE standard for MAC addresses. FakeAP is an active MAC searching tool, that broadcast a dummy beacon to trick the hacking scripts into identifying itself. Other tools also employ MAC address conflicts.

A possible solution to limit access of Linksys is to physically disable one of the two RF antennas on the router. This solution is based on the principle of "what is not seen or sensed may not exist". If the physical range of the router is decreased significantly, then no one outside the range would detect that there is a wireless router. The disadvantages to this approach is that it disables diversity signaling (for reliable communication over weaker signal strength) and that the router range cannot be customized to the contours of the office. A detailed analysis on other methods to physically limit signals will be discussed later.

In summary, the built-in features provided by Linksys provide minimal security for the wireless network. These security mechanisms prevent accidental access to the network and casual network attack. The wireless network is bare and vulnerable to more sophisticated attacks made available through tools over the Internet, like Wellenreiter or AirJack, or even tools provided by the network card manufacturer itself. Other countermeasures must be used in order to secure the network.

III. Vulnerability of WEP algorithm

The main problem that makes 802.11b based wireless network vulnerable to attack is its encryption protocol – Wired Equivalent Privacy (WEP). It is defined in the IEEE 802.11 standard with the goal of preventing eavesdropping. However, it did not consider the problem of authorization and that results in security vulnerability. Although one can use WEP as some form of authorization by keeping the key secret, flaws in the specification hinders the effectiveness of WEP in such role.

A. The Problems

The 802.11 specification is vague in the implementation, and flaws in the design; therefore, it makes systems easy to exploit by intruders.

The implementation uses an algorithm that utilizes RC4 stream cipher for encryption and CRC-32 checksum for integrity check. If the same key is reused, it is possible for an eavesdropper to find the XOR of two messages and perform a statistical analysis on the result. The WEP protocol attempted to remedy the problem by using an Initialization Vector (IV) is used to produce a different RC4 encipher for each packet sent.

Although Initialization Vector (IV) is a good idea, WEP uses only a 24-bit IV field. In addition, the 24-bits are sent in clear text through the wireless network. Thus, if an eavesdropper listens for an extended period of time, he may be able to build a dictionary of all IV key streams. A rough calculation done by Borisov, Goldberg, and Wagner suggest that will take about 15 gigabyte of memory space to build such a dictionary.

Addition, the use of CRC-32 as integrity check also allows attackers to modify the message as if it was genuinely correct. Since CRC-32 algorithm is linear, changing a bit in the message would change specific checksum bits declared by CRC algorithm. Therefore, the attacker simply alters the checksum to appear as if the integrity has not been compromised..

B. Common Implementation Flaws

Even though there are fundamental flaws in the implementation of WEP, the main problem is with how the system administrator implements the network. For the convenience for both system administrators and end users, often a network uses the same pre-shared key for every access point on the network and mobile station. For an eavesdropper, it is easy to compute the shared key by analyzing the massive amount of traffics that occurs in a short time.

Assuming a typical busy access point which consistently send packet at the size of 2000 bytes at 11Mbps, it would take 2000*8/(11*10^6)*2^24 ~= 24400 seconds, or roughly 7 hours to build the IV dictionary, In many instance the packet size is much smaller than 2000 bytes, which would complete the job much faster. Essentially most large wireless network could be “accessed” in a day’s time.

C. Attacks

1) Predictable Plaintext in Encrypted Text

One reason that the encrypted text in 802.11b sent message is easily breakable is that it is rather easy to predict the content. Most packets sent by wireless are IP packet, where the header contains a lot of redundancy, using which a hacker could easily guessed the content. Armed with the knowledge of the pattern of a typical IP packet, one can easily perform statistical analysis on the captured text to get the cipher key.

2) Hardware Design Vulnerability

Listening and capturing packet in the 2.4G band is rather difficult but modifying existing equipment for doing the task is easy for an experienced attacker. Theoretically, all commercial 802.11b equipment is designed to filter out messages that it does not have the encryption key for. However, if the equipment is alters, it could be used to passed back encrypted packet for analysis. Most commercial 802.11b equipment on the market comes with a programmable firmware, designed for future upgrade or performance enhancements. Therefore, a hacker could backward-engineered the firmware and load it into the hardware and the device would be an excellent tool. Although backward-engineering the firmware takes a long time, it is only one time work and it can be collaboration work from hackers around the world.

3) Rerouting Packets

Armed with the knowledge of IP packet, it is possible to capture and inspect the data of the network without modifying any hardware. Since most wireless network are interconnected to the internet, and the location of the IP address in the IP packet is fixed, one can manipulate the byte in that packet to make it send to a rogue server on the internet for further analysis.

D. Overhead and Speed

Even though WEP is flawed in the security sense, it still provides basic forms of authentication and encryption for data. However, many of the wireless network deployed, mainly private networks, do not even have WEP enabled.

There are two reasons for such an occurrence. Firstly, it is considered troublesome to remember the encryption key for the system (which is usually 40 or 128 bits). Secondly, WEP overheads decrease performance.

Below is a small empirical experiment on the WEP impact on speed using the Linksys BEFW11S4 802.11b router, Linksys WPC11 Network card, and downloading a 605mb files from the internet under the same network conditions:

TABLE I

WEP Overhead Impact on Performance

	Download Time
With 128 bit WEP	38 minutes
Unsecured	18 minutes

From the data above, using WEP would have a 53% speed impact. For some networks that have to deal with large amount of data transfer, is an unacceptable overhead for the security it provides.

E. Improvements

An attempt to improve WEP security is made by the 802.11 Task Group in preparation for the future 802.11i standard. WPA, or Wi-Fi Protected Access, is basically a combination of WEP with Temporal Key Integrity Protocol (TKIP). TKIP uses a master key as a starting point, and derives subsequent keys for which would be changed periodically. The problem with WPA is that older 802.11b equipments do not provide support for it and thus, the hardware automatically downgrades it to WEP – rendering the implementation useless.

F. Conclusion

The problems faced with WEP encryption come from both flaws in design and imperfections in implementation. Due to the lack of specification in the 802.11 standard, WEP is mostly implemented with a fixed shared key. For a large deployment of wireless networks, it provides too much raw data for the intruder to analyze. The linearity of CRC-32 also opens the gate for intruders to exploit – combined with the predictability of the data and the enormous overhead of the WEP scheme, results in security vulnerabilities in WEP systems.

IV. Solutions

A. Utilization of VPN technology

VPN, or Virtual Private Network, is primarily used for creating a secure channel between two private networks through an insecure or public network. While the technology is primarily intended for the Internet, it is possible to create a secure link in an insecure wireless network. Two of the most common used algorithms used to encrypt VPN channels are IPsec and PPTP.

1) IPsec

IPsec, also known as IP Security, is a framework of open standards for ensuring secure private communications over IP networks [5]. The main concept behind IPsec is a technique called tunneling, which encapsulates an IP packet within another IP packet. It has two modes of operation: tunnel mode and transport mode. The tunnel mode encrypts the entire IP packet, header and payload, and reveals only the IP address of the IPsec gateway. The transport mode, however, encrypts only the payload sections and allows the IP header to be read.

For confidentiality, IPsec encrypts IP packets using the Data Encryption Standard (DES) or variants of it [7]. DES uses a 56-bit key and has been in use for about 20 years. However, DES was compromised in 1999 within 23 hours during a competition [8]. Therefore, modern IPsec employs the Triple DES (3DES) or the Advanced Encryption Standard (AES). Triple DES encrypts the data three times with up to three different keys and AES is a new 128-bit algorithm that is faster and more secure than DES or 3DES.

2) PPTP

PPTP is an open-documented standard published by the Internet Engineering Task Force (IETF) as RFC 2637PPTP. The theory behind PPTP tunneling is similar to that of IPsec, but PPTP tunneling uses a different scheme and it only allows tunneling mode. The most commonly used PPTP implementation is a proprietary implementation developed by Microsoft for its NT VPN services.

Microsoft PPTP combines with Challenge Handshake Authentication Protocol (CHAP) and Microsoft Point to Point Encryption (MPPE) to provide both authentication and encryption for client accessing the network. While the CHAP protocol proven to be flawed, the new version of CHAP (MSCHAPv2) have been proven to patches the flaw of the algorithm.

3) Advantages and Disadvantage of VPN

The advantages of VPN over WEP are that it provides authentication for individual users rather than sharing one encryption key. The 3DES and MPPE encryptions, employed by the IPsec and PPTP protocol respectively, are both much harder to crack than the WEP native standards. Presently, no one has claimed that they have cracked the 3DES or PPTP using MSCHAPv2 encryption. The overhead for VPN is also much smaller than those for WEP. A study done in Japan suggests that MPPE gives only a 25% speed penalty on 128-bit encryption.

The problem with VPN is that it requires a central server to handle authentication and mediate the data communication. PPTP is available as a part of Microsoft Windows Server, and is available as a free solution with Linux, and most hardware VPN solutions employ IPsec, along with solutions from UNIX/Linux servers. However, a weakness in this solution is that VPN protects the integrity and security of the data transmitted on the network, but it does not secure the channel. That is, an intruder can still access the wireless network bandwidth and could potentially launch a denial-of-service attack by significantly increasing traffic until the legitimate connections cannot send or receive any data.

4) IPsec or PPTP

Although both IPsec and PPTP are both VPN implementations, they are not compatible with each other, and require different VPN clients in order to establish connections to the respective network. Windows provides a built-in VPN dial-in system, but it only supports the Microsoft PPTP implementation. IPsec support on the Windows VPN would require a rather complicated setup procedure. Thus, most Windows users use third-party VPN software such as GreenBow, Sentinel SSH or other IPsec clients that come with hardware VPN solutions.

In general, VPN provides much better security than WEP. It gives better authentication capability, improves data encryption and confidentiality, and gives a lower performance penalty. The solutions come at the expense that a dedicated server is necessary to handle the traffic. Nevertheless, this is a better solution than what WEP offers.

B. Physical Signal Limitation

One of the ways to deal with security issues of WLAN is to tackle it at the physical level. The WLAN signal for 802.11b is a radio frequency operating at 2.4GHz. Therefore, there are two ways to limit the signal from reaching physically insecure areas: signal jamming and signal directing.

A signal jammer is a device that prevents any signals from passing through its designated area and operates “by occupying [the entire] available spectrum within its range” [9]. The key to its operation is the creation of jamming signals that interferes with regular WLAN signals such that any unauthorized connections will be interrupted. Clearly, signal jammers has an advantage over regular, non-protected WLAN signal in that it prevents signals from reaching an unintended area. In addition, compared to other implementations that secure WLAN signals, signal jammers are easy to implement and requires little technical skill. To setup a signal jammer, one simply has to purchase the device and power it on. Unfortunately, signal jammers are not as ideal as it appears, and it may not be legal in some countries. Signal jammers are not specific in area or signal and therefore, cannot pin-point specific signals to jam. Thus, the jammer may potentially affect other wireless communication devices operating on the frequency, like cordless phones. These unintentionally blocked devices may be a crucial resource within a small business environment. Similarly, signal jammers are not able to provide a clear physical area to block signals. Therefore, one must rely on the placement of signal jammers to create a boundary. However, that is extremely difficult since the original design of signal jammers is not to define an area to limit signals, but rather to prohibit the use of wireless devices within an area. Furthermore, this might also mistakenly jam the signals of other businesses. Another issue with signal jammers is the cost. Current market price of signal jammers range from hundreds to even thousands of dollar and purchasing many of such devices is clearly unfeasible. An example of such devices is a “2.4 GHz [signal] jamming device… that will block video the signals of wireless cameras, wireless LANs and Bluetooth” but at cost of £189.99 (CAD $423).

Alternatively, signal directing shows much promise. The idea behind signal directing is redirecting the signal direction and limiting signal range. Similar to the signal jamming, signal directing can prevent unauthorized access of WLAN on a physical level by preventing access in undesignated areas. However, the fundamental implementation differs in that, instead of generating a jamming signal, a conductive material such as aluminum is placed between the links to absorb the signals. One possible method of applying this technique is to enclose the desired WLAN area with a Faraday cage. “A Faraday cage is an enclosure with no apertures (holes, slits, windows or doors) made of a perfectly conducting material” [10]. Even though an ideal Faraday cage is not possible to be built, using the idea to design a room with similar functionality is possible. A room which can block signals can be constructed by “lining the walls with aluminum foil, and using glass that absorbs radio waves in the windows” [11]. However, this method suffers similar drawbacks as signal jamming in that it absorbs all signals coming in and out of the area such as mobile phone signals and even AM/FM radio signals. Furthermore, it is even more costly than signal jammers to renovate the entire business area to install aluminum foil walls and the radio wave absorbing glasses. Nevertheless, there are alterative methods of implementing signal directing for small businesses. Instead of having a Faraday cage for the whole room, one can use the conducting material to absorb the signal at the wireless access point. Unlike the Faraday cage, however, only parts of the access point will be covered and that allows the uncovered areas to continue transmitting the signals. Therefore, it is not difficult to control the direction of the signals only to the direction desired. Furthermore, this kind of signal directing method has a great advantage on the cost front because such material can be found for a low price. For example, one possible material is an ordinary aluminum insect screen [12]. Because the installation process is simple and the cost is simply a roll of aluminum insect foil [12], this design certainly has its advantages. Nevertheless, it has its drawbacks in that the signal is not guaranteed not to escape the desired area due to the fact that the range cannot be finely manipulated. Moreover, the most materials, like the aluminum insect screen, are not the most ideal material and allow signals to penetrate it. Regardless, the signals are weakened enough such that it cannot pass through other obstacles.

Using the similar concept, BAE developed a high-tech wallpaper, known as the “anti-Wi-Fi wallpaper ” that prevents wireless signals from passing through. However, it differs from signal jammers or signal directors in that it allows mobile phone signals through. The principle behind this technology is the use of “an optical diffraction grating [that creates] interference to destroy certain light frequencies” [11]. The filter for the wallpaper can be enabled and disabled at anytime, making this the technical choice to solve the problem. This technology came with a high cost of about £500 (CAD $1100) per square meter, which is more expensive than any other solutions in the market. It is obvious that a small business cannot afford to use this technology.

Depending on the budget and the desired security level, a business can have several options in terms of physical signal limitation. There is a constant conflict between the cost and the security level for the implemented solution. Often, obtaining a high security solution implies a higher cost. For the budget-minded businesses, the insect-screen design is a cost-effective solution to minimize signal bleeding, but it is often difficult to tune and might not completely block the signals outside the desired boundary. At the highest cost, the wireless-filtering wallpaper has the best security levels as well as the most flexibility. The midrange solutions, like the jammer, offer high security levels and little flexibility.

V. Implementation

The solutions mentioned above vary in cost and security level. For a small business like MedInstrumentCo, the budget allocated for computer security may not cover even one percent of what large companies consider a light security configuration. Therefore, the solutions will have to be scrutinized for price and cost effectiveness. The following proposed implementation of the solutions are targeted at under CAD $500. In all cases, the recommended router- provided solutions should be used to prevent casual wireless network access, with the exception of WEP.

A. Hybrid Network – Wired and Wireless

This solution is provides use of some wired security and wireless freedom. It is also a cost-effective and reliable method to secure the wireless networks based on network segregation. However, there is a complicated set of rules that will dictate how users of the system will use the network.

Network segregation can be used so that the confidential patient records are on an isolated network connected only with wires, and placed upstairs. The customer database server will reside upstairs as well, with a physical wire running from upstairs to downstairs connecting with the PoS equipment. The PoS and inventory equipment may connect with each other via the wireless network if it will not be used to transmit confidential data or transaction records. Development computers containing proprietary data will be kept either on a third network, or carefully integrated with the confidential patient record network upstairs. The latter solution will assume that precautions are taken to prevent any patient data from being exposed in published business documents.

The rationale behind this solution is that the owner of MedInstrumentCo should understand that the benefits of using wireless must outweigh the troubles and security risks taken to deploy the wireless network.

B. *Software VPN server (on dedicated computer)*

This solution does not inherit the complications of the wired/wireless hybrid model of solution 1. It offers flexibility and would make use of the current equipments, wireless router and network cards, that MedInstrumentCo has already. The patient records, company data, and customer database server and can be arbitrarily placed and would be reasonably secured, though at a risk that one day someone has cracked the encryption cipher. Note that we will assume that precautions are taken to prevent human error or negligence from accidentally disclosing the confidential data to the public and from each other.

The cheapest implementation will be the use the VPN software that comes with the operating system, like the VPN server built-in to Windows Server, or the open-source Linux VPN solutions. Since small businesses often do not use multiple operating system platforms or access other VPN networks besides their own, buying other VPN solutions may not be a good investment unless they come packaged with desirable features like improved authentication (e.g., RADIUS with LDAP or Kerberos).

To prevent access to the wireless channel provided by the wireless router, the most effective and lowest cost solution is to use the “aluminum insect-screen wrap” solution, where the range can be limited by the shape and thickness of the wrap material. However, this is cumbersome to implement, and requires several iterations of surveying the network perimeters with a notebook computer.

C. *New Security-Enhanced Wireless Router*

This solution is often neglected, as society tends to “patch up” existing systems instead of scrubbing clean the system. Though this is often thought of as wasteful and it costs more initially, it provides a convenient all-in-one solution, and could cost less than both solutions mentioned previously. An example of this would be that this solution does not need for a dedicated computer to run the VPN server, and the enhanced router would consume much less power than the operation of network switches and computer servers used in the other solutions. Combined with the “insect screen” solution, it is comparable to the other two solutions.

Examples of the enhanced security aspects of the router would be built-in VPN, intrusion detection, and authentication server, but is priced at CAD $300, which is three times the cost of a traditional wireless router.

The major drawback to this solution is that if a single security mechanism is compromised, such as an authentication backdoor, then the entire router and wireless network compromised.

VI. Recommendation

The most secure implementation would be the combination of implementation one and two if data transferring between the various networks are minimal, and that the policies to ensure data confidentiality are established. Implementation two is perhaps the most secure, but requires is only recommended for knowledgeable and experienced users in the small business. Limited to the scope of the owner of the small business, the third implementation is the recommended choice.

VII. Appendix

Cost to Build a Network

Option 1: Hybrid Wireless and Wired

Product	#	**Price**	**Total**
Router			
Linksys BEFW11S4 Router	1	$72.24	$72.24
Network Card			
Linksys WMP 11 PCI Wireless Network Card*	6	$63.21	$379.26
Linksys LNE100TX 10/100 LAN PCI Card	4	$26.52	$106.08
Network Cable			
RJ45 10FT CABLE Cat 5e	4	$2.98	$11.92
		Total:	$569.50

*Same price for USB units

Option 2: Full Wireless Network

Product	#	**Price**	**Total**
Router			
Linksys BEFW11S4 Router	1	$72.24	$72.24
Network Card			
Linksys WMP 11 PCI Wireless Network Card*	10	$63.21	$632.10
		Total:	$704.34

*Same price for USB units

Option3: Full Wired Network

Product	#	**Price**	**Total**

Router and Switch			
Linksys BEFSR81 Router	1	$107.97	$107.97
Linksys EFAH08W 8-port Switch	1	$75.46	$75.46
Network Card			
Linksys LNE100TX 10/100 LAN PCI Card	10	$26.52	$265.20
Cable*			
RJ45 1000FT CAT5E ETHERNET CABLE (Bulk)	1	$73.53	$73.53
RJ45 Modular Plug	24	$0.38	$9.12
RJ45 Wall Mount Connector	2	$1.00	$2.00
Labour			
Wiring between the two floors (Professionally done)	1	$50.00	$50.00
		Total:	$533.28
		With Labour:	$583.28

***10 cables, 2 each, 2 more cables for hub to hub

Cost to Add Additional Connection:
Wireless:

Product	#	Price	Total
Linksys WMP 11 PCI Wireless Network Card*	1	$63.21	$63.21
		Total:	$63.21

***up to 255 total connections

Wired:

Product	#	Price	Total
Linksys LNE100TX 10/100 LAN PCI Card*	1	$26.52	$26.52
Cable	1	$2.98	$2.98
		Total:	$29.50

*up to the switch limit

Network analyzed under these conditions: 10 computers, 6 upstairs, 4 downstairs, internet connection is located downstairs in the same room as the 4 computers. No labour cost for user setup-able components. Labour costs are $50/hour if done professionally. All computers do not have a network card initially.

Analysis: The cheapest option, after labour, is to have a wireless and wired hybrid, the most expensive option is to go for all wireless solution, the wired solution is similar in price to the hybrid system. Also the cost of expanding network is not the same, for wireless it is consistent, but for wired network, new switches are needed after adding a set amount of connections, usually 5, 8 or 16.

REFERENCES

[1] Linksys. “Application Note: Important Information for Wireless Products”. Linksys BEFW11S4 version 3.2 retail package documentation. (Irvine:Cisco Systems, 2003). Accessible online. “Important Information on Wireless & Security”. (Irvine:Cisco Systems, 2003).Online. Linksys. Internet. 17 Oct 2004. <http://www.linksys.com/splash/wirelessnotes.asp>

[2] Wilson, J. “SSID differences”. Online posting. 02 Feb 2003. Experts Exchange. 21 Oct 2004. <http://www.experts-exchange.com/Programming/Wireless_Programming/802_11x_User/Q_20493147.html>

[3] Moskowitz, R. “WLAN Testing Reports: Debunking the Myth of SSID Hiding”. Online. 01 Dec 2003. ICSA labs. 11 Nov 2004. <http://www.icsalabs.com/html/communities/WLAN/wp_ssid_hiding.pdf> Page 3.

[4] Wright, J. “Detecting Wireless LAN MAC Address Spoofing”. Online. 22 Jan 2003. Linux Security. 16 Nov 2004. < http://www.linuxsecurity.com/articles/documentation_article-6585.html>. Article hosted <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>. Page 4.

[5] Godber, P. “Secure Wireless Gateway,” WiSe, September 28, 2002, Atlanta, Georgia, p41 – 46

[6] Baghaei, N.; Hunt, R. “Security performance of loaded IEEE 802.11b wireless networks,” Computer Communications, v. 27, July 6, 2004.

[7] Convery, S.; Miller, D. “SAFE: wireless LAN security in depth, version 2. White paper”, Cisco Systems, Inc, 2003, http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf.

[8] Halpern, J. “SAFE: VPN IPSec Virtual Private Networks in Depth”, White Paper, Cisco System, Inc, 2004 http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml

[9] "Web BSNL Portal || Telecom Guide," [Online document], 2004 Aug 10, [cited 2004 Nov 20], Available HTTP: http://www.bsnl.in/Telecomguide.asp?intNewsId=39079&strNewsMore=more

[10] "BOLT - Discussion of Faraday Cage," [Online document], 2004 Aug 10, [cited 2004 Nov 20], Available HTTP: http://www.boltlightningprotection.com/Elemental_Faraday_Cage.htm

[11] Fox, B. “Stealth wallpaper keeps company secrets safe," [Online document], 2004 Aug 8, [cited 2004 Nov 21], Available HTTP: http://www.newscientist.com/news/news.jsp?id=ns99996240

[12] Kroll, D.; Sowell, G. “Stealth wallpaper keeps company secrets safe," [Online document], 2004 June 16, [cited 2004 Nov 21], Available HTTP: http://www.extensiontech.net/articles/howto/gs/wifiblock/

[13] De Clercq, J.; Paridaens, O. “Scalability Implications of Virtual Private Networks,” IEEE Communications Magazine, May 2002, p151-157

[14] Schneier, B. “Cryptanalysis of Microsoft’s point-to-point tunneling protocol (PPTP),“ in 5th ACM Conference on Computer and Communications Security, 1998, p 132-141

[15] Ramsey, M. “PoPToP, a Secure and Free VPN Solution”, Linux Journal, June 2000

[16] Masuda, H.; Nakanishi, M. "Secure wireless LAN service at a COOP cafeteria" Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on , Volume: 2 , 28-30 Aug. 2003 Pages:704 - 707 vol.2