Information Security Management: A Research Project

Pramod Pandya and Reza Frazin
California State University, Fullerton, CA 92834, USA

ppandya@fullerton.edu rfrazin@fullerton.edu

Abstract

In an environment of growing information security threats, it is essential to raise the awareness and capabilities of business students entering the workforce to mitigate threats to the enterprise networks. Information security has emerged as the most critical component of any data network. This paper describes a research project jointly undertaken by the author and an undergraduate student in Information Systems to explore some of the technical aspects of information security over the wired and wireless networks.

Keywords: Network Security, virtual private networks, encryption, wireless networks

Introduction

The next step in the evolution of enterprise networking is the wireless LANs, which are being deployed across all industries, including Financial Service Providers for their productivity and cost-saving benefits. Corporate responsibility dictates the need to secure data from unauthorized access, such as competitors, hackers, and other security threats (Computer Security Institute and Federal Bureau of Investigation, 2002). The growth of information systems and in particular e-commerce activities over the Internet has increased the risk to corporate data, and thus assurance of information and data communications infrastructure is of paramount importance. Information security has become an exciting topic of discussion in the popular computer and networking technical journals. The skills required to investigate, manage, and respond to cyber attacks are sought by Fortune 500 corporations. Hands-on projects, which are technical but simple to implement, can help motivate the Information Systems (IS) students to explore the technical concepts of information security. The research project undertaken by the IS undergraduate student is simple enough to implement, as it requires just elementary programming skills. Furthermore, the project provides the undergraduate student to explore in some depth, some of the technical aspects of information security. The UNDERGRADUATE SUPPORT INITIATIVE funded the research project under RESEARCH/CREATIVE AWARDS sponsored by Faculty Development Center at California State University, Fullerton. The award money was budgeted for hardware, software and the undergraduate student time.

Project Definition – Learning Objectives

The project will provide hands on experience to the IS student with limited technical background while requiring limited technical support. The scope of the research project was to explore the strengths and weaknesses of net-

work security. Hence, we decided to focus on a series of commonly used technologies and methods, which can provide a substantial, secured network environment. The four aspects of project included:

- Network security via Virtual Private Network using Vtun software
- Network security via Virtual Private Network using LinkSys router
- Wireless Security using WEP, and MAC filtering
- Network vulnerability and securing network from intruders.

A virtual private network (VPN) is an extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables one to send data between two computers across a shared or public inter-network very similar to a point-to-point private link rather then a shared network, which could expose the data being communicated, to anyone who shares the connection medium. First a VPN circuit is setup, next the data is encrypted and a header is added to provide routing information, thus allowing data to traverse the shared or public inter-network to reach its endpoint. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. There are two major classes of encryption algorithms (Forouzan, 2003b): symmetric and asymmetric encryption. Symmetric encryption uses one secret key for both encryption and decryption. The message sender and the recipient share this key. Some popular conventional encryption algorithms are Blowfish (Schneier, 1993), RC5 (Rivest, 1994), and DES (FIPS, 1977). Public-key encryption (asymmetric encryption) has two keys. One key (public key) is used to encrypt the message and a second, very private key is used to decrypt the message. The most popular public-key algorithm is the RSA encryption algorithm (Rivest, Sharmir, & Adleman, 1978).

Project as a Pedagogical Tool

The final report should include a discussion on information security concepts that were learnt by having analyzed the outcomes of the project. Those concepts include the following:

1. Understand the danger of wiretapping and the importance of information security when messages are passed between the client and server computers.

2. Discuss the method used by the client and the server computer to encrypt and decrypt the message.

3. Understand the differences between the encryption method used in the wired and the wireless data communication.

An Overview of Tunneling Software

There are many software packages that enable users to create tunnels and setup VPN's. We decided to use a freeware (Vtun http://vtun.sourceforge.net/), open source software written for the Linux operating system from SourceForge.net, the world's largest
Open Source software development website, with the largest repository of Open Source code and applications available on the Internet (Schiffman, 2003), (Russell, Boar, & Eller, 2000). The user must install and configure Vtun software. The configuration file determines how Vtun operates, either as a Vtun server, which can then accept connections from Vtun clients, or as a Vtun client, which can then establish a connection to a specified Vtun server.

The configuration (Config) file consists of a series of settings such as the tunnel type being used, in our case we are using IP tunneling, other supported tunnel methods are Ethernet, and Serial. The Config file must also include the type of protocol to use; in our case we are using TCP. This

is done by including this line “proto tcp;” Other major parts to the config file are the session name and password that is to be used on the host. But the main part of the config file is the addressing that needs to be established within our tunnel network. We chose two private IP's for each client (10.0.0.1, 10.0.0.2). The next step was to execute the Vtun program with the appropriate commands to create the tunnel connection. The basic syntax for the Vtun command line is as follows.

To run Vtun as a Server:
vtund <-s> [-f file] [-P port]

To run Vtun as a Client:
vtund [-f file] [-P port] [-L local address] [-p] [-t timeout] <host> <server address>

Vtund <-s> establishes Vtun as a server, -f is followed by the pathname to the location of the configuration file, and –P refers to the TCP port on which the server would setup a link with the client. In our project the server is running on port 5000. The next list of command line focuses on the client portion of Vtun. The -f (location of the configuration), -P (the port address running on the server), the server address is the IP Address of the server. In our project the command line was based on “vtund -P 5000 -f /root/vtun/vtund.conf 4.35.41.10”. When Vtun is invoked as a client, it can establish a link to a Vtun server, provided it is authenticated by the server. The command “ifconfig” is used to display current network connections and the settings. Once the link is established, client connects to the server creating a virtual private tunnel, thus enabling to communicate over the point-to-point link through the Internet.

An Overview of Wireless LAN

In 1997, the first internationally sanctioned wireless LAN standard, 802.11 was approved by IEEE. This standard proposed two type of implementation for the physical layer (OSI layers) that is:

> Radio frequency (RF) signaling in the 2.4 GHz band using frequency hopping spread spectrum (FHSS)
>
> Radio frequency (RF) signaling in the 2.4 GHz band using direct sequence spread spectrum (DSSS)

Further developments were made on the original 2.4 GHz band, and the 802.11b standard was established in 1999, which was to deliver raw data rates up to 11 Mbps. A wireless LAN extends the limited reach of traditional wired networks inside a building by enabling network communications to occur over the air. In the office environment, a wireless network offers end-users the benefits of increased mobility and increased productivity, because it enables mobile users to access information and network resources as they attend meetings, collaborate with other users, or move to other locations in the office. Cometa Networks (http://www.cometanetworks.com) founded by IBM, AT&T, and Intel in December 2002, provides wholesale Wi-Fi (the 802.11 standard set) Internet access services to wireless carriers, Internet service providers, and other telecommunications providers that want to offer secured, robust public Internet access to their enterprise and retail customers.

Project Implementation

Wired Network Security Issues

Configuration of Vtun software on Linux based platforms was carried out by the student, so that the student can get acquainted with installation of operating system. The details of TCP/IP network design were jointly undertaken by both the authors. With the setup so far, we were able to

set up a VPN among three locations using Vtun software. As a follow up to setting VPN using Vtun, we use the LinkSys router at each of the three locations to repeat the experiment.

The project accomplishments included setting up a VPN to achieve a secured private data link among three public locations. We demonstrated that by using specialized software and hardware such as Vtun and LinkSys router, a secured connection could be established over a public wired network. A VPN is a secured (SSL, 2003), private communication tunnel between two or more devices across a public network (like the Internet). VPN devices can be either computer running VPN software, or a special device like a VPN enabled router (Linksys router). Commercial grade software enables the user to configure VPN traffic to Internet sites with more than one Internet link (Proficient Networks, 2003).

Wireless Network Security Issues

The Hacker's Wireless LAN Toolbox, is a collection of software tools to scan and break the 802.11b protocol, and is freely available on the Internet for both the MS-Windows and Linux operating system. White Papers on Wireless LAN Security are readily available from Air Defense, Inc. web site (http://www.airdefense.net), which provides a comprehensive write up on tools to hack, and monitor the Wireless networks. The next phase of our project was to investigate network security features of IEEE 802.11b wireless network (Pahlavan & Krishnamurty, 2002). The research showed the current methods of Wireless encryptions methods are insecure and vulnerable. Wired Equivalent Privacy (WEP) standard is used to encrypt data between the client computer and the access point. (Wired Equivalent Privacy (WEP) is a security protocol, specified in the *IEEE Wireless Fidelity (Wi-Fi) standard*, 802.11b.) It is important for WEP encryption that each packet transmitted must have a different WEP key. While the WEP standard had specified use of different keys for different data packets, the key derivation function (how to derive a key from a common starting point) is flawed. The keys for different data packets are too similar. Hence a hacker could exploit this similarity to extract information about the key, after having analyzed a modest number of packets. Once the key is discovered, a malicious hacker could decrypt data packets being passed along the exposed network.

Our next activity was to scan for wireless data networks at random in a neighborhood. We refer to a paper that deals with mapping of wireless access points, presented at a conference organized by USENIX (Simon, 2002). There are numerous discussion papers available on the Internet that deals with the subject of mapping and pin-pointing the exact locations of wireless access points (Clegg, 2002). However this does raise an ethical issue, but we felt that as long as we were not planning to hack into unsecured wireless networks, this ought not to create a problem. Therefore, we decided against identifying and notifying the owners of the unsecured networks. We discovered that a wireless network called "Mac home" was available, but it was WAP protected. Wireless Application Protocol (WAP), which we will discuss later, is the encryption algorithm used by the wireless industry. (WAP is published by the *WAP Forum*, founded in 1997 by Ericsson, Motorola, Nokia, and Unwired Planet. As we moved on throughout the neighborhood we were able to pickup ELEVEN more wireless networks, a total of 8 networks were left without any WEP, Media Access Control (MAC) address filtering or other security measures (Forouzan, 2003a).

The significant information that we captured while scanning the wireless network included the router's Service Set Identifier (SSID). A router's SSID identifies the manufacturer of the router, which in turn enables a hacker to gain access to the router if the factory set password had not been changed. Each manufacturer will set a password for users to access the router for the first time. It is the responsibility of the user to change this password. One of the strongest points that has helped the surge in sales of wireless devices has been claims by manufactures such as "ready to go out of the box", and "one step setup". Users are not aware of this security hazard. An unse-

cured network opens network to any person who has a wireless enabled device such as a laptop or a hand held device.

Security Guidelines for Wireless Network

The learning objectives regarding the security aspects of data over the wired and the wireless networks were met. We now have a much clearer understanding of wired and wireless networks. Valuable lessons learnt from this project and the corrective actions are presented below.

Change the Default Password

Almost all wireless devices can be managed via a web interface that can be accessed by simply typing its IP address in a browser's address field. While the admin interface is password protected, the default password set by the manufacturer is always the same. Any wireless network sniffer program will easily discover the manufacturer of the wireless device because it will broadcast that information. As a result, an intruder can type in the default IP address of the wireless gateway to get to the admin interface, and try the default password to log in and access the device settings. The manufacturer of the device gives the intruder the additional benefit of being able to exploit vulnerabilities specific to that manufacturer.

Disable SSID Broadcast

The SSID is the name of the wireless network. In order to connect to a wireless network, its name needs to be known. By default, wireless gateways broadcast the SSID, so it can easily be picked up by any wireless network device that is monitoring for a wireless data network. Hiding the SSID by disabling SSID broadcast will make it much harder for an intruder because he or she will have to start guessing. It may be worth mentioning that while most wireless gateway devices offer the option to disable SSID broadcast, some devices require a firmware upgrade, and some devices do not offer that option at all.

Change the SSID

Disabling SSID broadcast does not help much if the SSID remains the manufacturer's default, which is just as easily found in the manual as the default admin password. The SSID should be changed to a custom phrase that is difficult to guess. The use of non-dictionary words as well as numbers and special characters for the new SSID is encouraged.

Enable Encryption

Wireless devices support the Wired Equivalent Privacy (WEP) with either 64-bit or 128-bit encryption. 64-bit encryption has been proven to be very weak and easily broken, 128-bit encryption is recommended because it is a lot more difficult to break (though far from impossible). Some devices might require a firmware upgrade to support 128-bit encryption. Encryption works by entering the encryption key on the wireless gateway as well as on the PC with the wireless card. All transmitted data is encrypted for the transfer between the two devices. If the encryption key does not match, the wireless gateway will not communicate.

In recent months the WEP encryption has been under heavy criticism due to its failure in protecting data. It is important for WEP encryption that each packet transmitted must have a different WEP key. While the WEP standard has specified using different keys for different data packets, the key derivation function (how to derive a key from a common starting point) is flawed. Simply, the keys for different data packets are too similar. Hackers could exploit this similarity to extract information about the key after having analyzed a modest number of packets.

Public domain software (Sniffer http://vtun.sourceforge.net), once installed on mobile systems, will recognize a wireless signal with WEP enabled, and will capture the data packets being transmitted between the Access Point and the client, even though the two devices are the only two that understand the encrypted data and know the password, due to WEP's weakness. Sniffer software can analyze the data and extract parts of the data until it has sufficient amount of information to make a guess on the WEP password.

Disable DHCP

Most gateway (router) devices by default have Dynamic Host Configuration Protocol, (DHCP) enabled. This means that any new host on a network that makes its presence known and broadcasts a request for an IP address will be automatically provided one with. However, this also makes it very easy for the intruder to connect to a wireless network. By simply setting the laptop to use DHCP, it will immediately receive all TCP/IP configuration information needed to connect to the network. While it is an inconvenience and requires more maintenance for the legitimate user, disabling DHCP and manually assigning static IP addresses creates another hurdle for the intruder. It requires to manually configuring the laptop with what the correct TCP/IP properties should be, being able to connect to the network (Forouzan, 2003b).

Change the Default Subnet

Disabling DHCP doesn't help much if the subnet remains the manufacturer's default, which is just easily found in the manual as the default admin password or SSID. Most devices use the common default subnet of 192.168.0.0 with a subnet mask of 255.255.255.0. The subnet should be changed to another private subnet. There are a number of non-routable IP address ranges that are reserved exclusively for use on private networks. These ranges are 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255 - plenty to choose from. This will prevent the intruder from assigning a static IP address and TCP/IP configuration information based on the manufacturer's default subnet.

Use Media Access Control (MAC) Address Filtering

Each network adapter has a unique hardware address also known as a MAC address. This hardware address is unique for each network card. Most wireless gateway devices support MAC address filtering. The way this works is that the legitimate user creates a list and enters only the MAC addresses of the network cards that are permitted to access the wireless network. Any network adapter with a MAC address that does not match a MAC address in the approved list will automatically be denied access to the wireless network. Only machines with authorized MAC addresses are allowed to participate in the network. A savvy intruder can spoof MAC addresses, but using MAC filtering is another good deterrent. Wireless LAN management software to monitor and identify unauthorized access points and users is available (Aruba, 2003).

Student Feedback

The undergraduate student was able to work with a variety of networking software and tools, as well as hardware resources such as routers, switches, and Wireless Access Points. These hardware and software resources are essential components for building private corporate networks. The main points reported by the student are listed below.

- The student was able to examine and detect unsecured wireless networks.
- Setup secured access to the wireless network.
- Understand the importance of protecting data to be transferred over the Internet.

- Obtained a better understanding of the basic mechanism of encryption procedure.
- This has led to a clearer understanding of the Open System Interconnection (OSI) model of data networking presented in a Data Communication class.

Conclusion

Development of a real secured information system is beyond the scope of an undergraduate IS student considering their level of technical competency. However, developing a simplified system is within their capabilities and affords them a deeper understanding of concepts than they might otherwise achieve. In working on this project, assigned tasks to the student were defined; guidance and supervision was provided to follow up research and implementation. The emphasis was for the student to be creative and devise an efficient means for performing research related objectives. The most important lesson we learnt from this project was that, the security issues related to wireless data networks have not been resolved. There has been much talk in the industry to resolve this problem and consensus on the next generation of encryption algorithm has been agreed. This new protocol is 802.11i, which is a replacement for the current Wi-Fi Protected Access (WPA) specification that Wi-Fi Alliance put forward in late 2002 as an interim replacement for the flawed Wired Equivalent Privacy (WEP) encryption standard. Our next project is to continue to investigate wireless network security using specialized software such as Intrusion Detection Systems (IDS) that would help to identify unauthorized ("rouge") access points, denial of service attacks (DOS), and improperly configured access points. Wireless intrusion detection systems work by continuously scanning an enterprise's airspace for the tell-tale signatures that indicate sophisticated DOS and man-in-the-middle attacks against networks secured by 802.1X-based authentication mechanism and/or VPN tunnels are underway. Explosion of wireless "hotspots" in public spaces, homes, and businesses has made the wireless network security more lucrative. Several IDS products are now available from Aruba Wireless Networks, IBM Corporation, and AirMagnet Inc.

References

Aruba. Wireless Networks, 2003. *Network World*, August 2003.

Clegg, A. (2002). The how and why of the RTP 802.11b mapping project. Retrieved February 28, 2004, from http://alan.clegg.com/802/802_mapping.html

Computer Security Institute and Federal Bureau of Investigation. (2002). 2002 CSI/FBI Computer Crime and Security Survey. *Computer Security Issues & Trends*, *VIII* (1), Spring.

Forouzan, B. (2003a). *Local area networks*. McGraw-Hill.

Forouzan, B. (2003b). *TCP/IP protocol suite.* McGraw-Hill.

Pahlavan, K., & Krishnamurty, P. (2002). *Principles Of wireless networks*. Prentice Hall.

Proficient Networks. (2003, August). *Network World*.

Rivest, R. (1994). The RC5 encryption algorithm. *Proceedings of Second International Workshop on Fast Software Encryption*, December 14-16, pp. 86-96.

Rivest, R., Sharmir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, *21* (2), 120-126.

Russell, R., Boar, B., & Eller, R. (2000). *Hack proofing your network*. Syngress Media.

Schiffman, M. (2003). *Building open source network security tools*. Wiley Publishing.

Schneier, B. (1993). Description of a new variable-length key, 64-bit block cipher (Blowfish), *Proceedings of Workshop on Fast Software Encryption*, December 9-11, pp. 191-204.

Simon, B. (2002). 802.11b Wireless AP Mapping. *BSDcon* 2002, February 11-14, 2002, San Francisco, CA.

SSL: The next-generation VPN. (2003, August). *Network World*.

Wi-Fi Protected Access (WPA). (2004) *Network World*, *21* (2).

Biography

Pramod Pandya, B.S., M.S., Ph.D., is a Professor in the Information Systems and Decision Sciences Department at California State University Fullerton. His research interests are in Data Communications, Probability and Information Theory, and Information Systems and Technology.

Reza Frazin is an undergraduate student in the Information Systems and Decision Sciences Department at California State University Fullerton. Reza's research interest is in security aspects of wireless data and voice networks.