Global Information Assurance Certification Paper

Wireless is not the Problem

Jack J. Couch
MCSE, CCDA, CCNA, MCT
Assignment Version #1.4b

Abstract

Wireless is not the problem. It is a wonderful technology that expands the limits of our access to the data we need. The problem is that this great advancement has been built on the shoulders of insecure infrastructures. The freedom of access wireless provides is nothing more than an additional and powerful doorway to these security feeble environments.

In this paper we will not be examining the WEP protocol. Much research has been done that proves WEP to be ineffective at achieving a reasonable measure of security; therefore it will not be discussed as an option. Instead this paper will explore the vulnerabilities in our current network infrastructures (wired and wireless), how these vulnerabilities would be mitigated in an ideal world, the barriers to achieving that ideal world, and finally the options available for minimizing the risks today.

Background

The recent addition of wireless technologies, and the lack of additional security features they provide, has brought intensified interest to the area of secure communication. This is not because wireless networks create new problems that must be solved, but because they provide expanded access to problems that have existed in wired networks from the beginning. In fact the problems facing administrators who wish to deploy wireless networks are likely the same problems they have been ignoring with their current wired infrastructure. Why then, if the problems are not new, is there so much interest in securing wireless networks? The answer to this question is the reason wireless networks are so desirable: a lack of physical boundaries. Not only can employees access the physical network from their desk, but also in the conference room, in the cafeteria, or even outside on a bench. This is a wonderful advancement in networking. With most 802.11b network devices connectivity is up to 100 meters via radio. This, however, means that anyone with a wireless card has physical access to your network, friendly or not.

To make matters worse many hackers have found how easy it is to turn a Pringles can into a wireless receiver antenna allowing for a 15 db gain providing connectivity at over a half mile! Now before getting too excited and shouting "Down with Evil Wireless", consider for a moment the fact that this open physical layer has absolutely no impact on the security of your communications,

but only on the accessibility to your communications. In other words, had your wired network been relatively secure with existing technologies that provide data integrity and confidentiality, the addition of a wireless segment would by no means be a significant security risk.

Unfortunately very few, if any, wired networks provide confidentiality and integrity to the data that traverses their veins. Instead these networks send traffic unencrypted and unsecured, and have always been "ripe for the picking." Our local area networks only saving grace has been that in order to connect to these gushy underbellies, attackers need physical access. However, even in wired networks some creative white hat hackers have found ways to gain just that through the use of a Dream Cast game console attached directly to the Ethernet network that opens a back door to the Internet. Other hackers simply find a way to use open ports in firewalls to gain control of a single box available via the Internet in order to gain physical access to the LAN. Now, thanks to wireless, this hurdle is unnecessary; physical access is available to anyone within at least 328 feet.

Attacks against your Network

Physical access must be achieved in order to attack a local area network. That is the reason that the most secure computer is one that is not connected to a network, has no keyboard, mouse or monitor, and is locked in a safe. That being said, the following discussion will assume that physical access is available either through an Ethernet tap, a wireless network, or through an Internet connection. Once physical access is gained there are three things that can be done to your network: "attacks on confidentiality, attacks on integrity, and attacks on availability" (Tripwire).

Confidentiality

Confidentiality attacks are, plainly put, designed to read the data as it passes by. In the case of unencrypted traffic, as is almost always the case on a LAN, the process is very simple. In order to read unencrypted data an attacker simply needs to perform a network "sniff." This means that the attacker places a network card in promiscuous mode, either manually or through the use of a user friendly tool such as Ethereal from www.ethereal.com, and copies all the data "off the wire." With this completed the attacker can, at his leisure, read all the data that flowed through a particular network segment. This often includes emails, web traffic, instant messages, file transfers, printing, passwords and a host of other potentially sensitive communications.

Integrity

Integrity attacks are attacks in which the data is modified in transit. The following is an excerpt from Day Two of the SANS Security Essentials course. It describes an integrity attack against communication flowing between Alice and Bob.

"…if he *(the attacker)* is feeling particularly mischievous he can stop direct communications between Alice and Bob and alter all the messages going back and forth. For example, if Alice says, "I'll buy 10 widgets at $10 each," the attacker can change that to, "I'll buy 100 widgets at $100 each." Then, when Bob replies, "That will be a total of $10,000" the attacker can change that to, "No problem, you can have them for free" (Cole).

Availability

Availability attacks attempt to prevent "…the systems responsible for delivering, storing and processing information *from being* accessible when needed, by those who need them" (Information Security Glossary). Denial of Service (DOS) attacks fall into this category. These attacks are often used to disable security countermeasures such as Intrusion Detection Systems (IDS) with the ultimate objective being compromise of sensitive data (a confidentiality attack), but can also be the sole purpose of the attacker, as in the case of the recent Distributed Denial of Service attacks against websites.

Wireless Access

These attacks are almost common place on both wired and wireless networks, but without physical boundaries wireless networks are easier targets. This is for a couple reasons. First, perimeter defenses are often avoided. When attacking a network from the Internet an attacker must usually subvert some type of perimeter defense, most often a firewall, but when attacking via a wireless connection such countermeasures are rarely deployed. Second, with a wireless network it is easier for an attacker to target a specific organization and even a specific department within that organization. If you would like to "sniff" data from the research and development department at company XYZ, you simply need to drive to the appropriate building and throw your Pringles can out the window. In order to accomplish the same task via the Internet an adequate network mapping would first need to be completed and possibly a number of perimeter defenses penetrated. Lastly, with a direct connection to the internal LAN availability attacks can make use of the full 11Mbps provided instead of the meager amount that would generally be achievable by other means. The "availability" that is being attacked can be that of a system, but is often simply stealing internet bandwidth for the attacker's purposes.

Public Key Cryptography

The best way to deal with the problem of confidentiality, integrity, and availability is through the use of PKI cryptography. Generally speaking when talking about cryptography, four services are in question, "Confidentiality, Integrity, Authentication, and Non-repudiation" (Menezes, Oorschot and Vanstone, 1.1). A quick overview of Public Key Cryptographic concepts is probably in order. There are six major components to a PKI (Public Key Infrastructure):

Public Key and Private Key - Each person using the PKI must be issued both a public and private key pair.

Certificate - The Certificate is a digitally signed electronic document that binds an individual to their public key. Each entity using the PKI must be issued one of these.

Public Key Algorithm - The Public Key Algorithm is the mathematical function that allows for encryption and decryption when used with the appropriate public or private key.

Hash Algorithm - The Hash Algorithm is a mathematical function that takes data and transforms it in such a way that it can not be reversed, but is unique.

Certificate Authority - The Certificate Authority is an entity that everyone using the PKI trusts to verify the identity of individuals that are issued Public / Private Key Pairs and Certificates.

Public Key Cryptography is based on a rather interesting mathematical function called a Public Key Algorithm. With this function two keys are produced, the public key and the private key. By encrypting data with the public key the data can only be decrypted with the private key. In the same fashion, by encrypting data with the private key the data can only be decrypted with the public key. With this amazing mathematical behavior it becomes possible to provide Confidentiality. This is achieved by encrypting data using the public key of the individual whom is authorized to view the contents. Only the corresponding Private Key will successfully decipher the data, therefore the data is kept confidential.

Another function used in PKI is called a Hash Algorithm. This is used for digital signatures, which provide Non-repudiation and Message Integrity. Non-repudiation means that you can't dispute that you engaged in a given transaction. It is very much like a hand signature. Theoretically your signature can be made only by you, and so if it shows up on a legal document, you can't claim that you didn't agree to the contract. With Non-repudiation services, electronic transactions are legally binding and indisputable. To create a digital signature a copy of the original document is run through a hash function. This

produces a hash, or message digest. With this Hash the original document cannot be recovered, but only the original document will produce the same hash. Then the signer's Private Key is used to encrypt the message digest. Both the original document along with the digitally signed message digest (digital signature) is sent to the receiver. The receiver now decrypts the message digest using the Public Key of the sender and runs the original document through the hash function again. If both resulting message digests match, verification that the document was signed by the sender and that it has not been modified is accomplished. Thus both Integrity and Non-repudiation has been achieved.

Authentication is the mechanism by which we verify that the individual accessing services is who we think he is. Authentication is essential to ensuring only authorized entities access a given service. To illustrate this point, consider a user, Bob, that needs access to a database service to retrieve contact information. If authentication is required, Bob must prove he is really Bob before gaining the access he seeks. On the other hand consider Sinbad (LOL), a hacker who wants access to the database to run a script designed to crash the system. Because Sinbad can't prove that he is Bob, or another authorized user, his inability to authenticate has prevented his availability attack. If it were possible for all resources to require effective Authentication all availability attacks would be prevented, barring those running under authenticated users credentials.

An Ideal World

Now before you start picturing a utopia where beer flows like water, and traffic is never congested, let me clarify. In order to fully provide integrity, confidentiality, and availability to our wired and wireless networks we must achieve end to end cryptography, to include encryption and authentication services. To solidify a clear picture of how these functions work, let's imagine that there is a global PKI that has been established and Frank, our fictitious friend, needs to gain access to resources that require participation in the PKI. The first thing Frank needs to do is contact the Certificate Authority and request a Private / Public Key Pair and Certificate. In this discussion we will say that the Department of Licensing has leapt into the 21st century and they are acting as the Certificate Authority. At this point it is the DOL's responsibility to verify that Frank is truly Frank, compute a Public / Private Key pair and publish Frank's certificate, containing his personal information such as name and address as well as his Public Key. The DOL would then issue Frank his Private Key (probably in the form of a smart card). That's it. Frank is ready to participate in the world of PKI. Let's say the first thing Frank decides to do is check his email using a wireless network connection. Since all communications are secured using PKI, wireless or wired is not an issue, Frank connects securely to his mail server and reads away.

IPSEC

The best way for Frank to make a secure connection to another machine is through the use of IPSEC. IPSEC is an existing standard and the following is a description of the process of establishing authenticated and encrypted communications using IPSEC compiled from Sheila Frankel's book "Demystifying the IPSEC Puzzle" and RFC 2409:

1. First Frank's laptop, named FRANK01, sends an ISAKMP SA (security association) initiator message to his email machine, Mail7. An ISAKMP session is the first of two phases required to establish an IPSEC connection. Franks initiator SA message, contains a number of proposed options for establishing the IPSEC connection including Encryption Algorithm, Hash Algorithm, and Authentication method. In this case Frank requests an ISAKMP connection using an Encryption Algorithm of either "Triple DES" or "Blowfish," a Hash Algorithm of "MD5," and a Authentication Method of "Public Key Original Mode."

2. Mail7 examines the SA sent and determines if the options for the Encryption Algorithm, Hash Algorithm, and Authentication Method contain acceptable choices, based on Mail7's configuration.

3. After it is determined that acceptable options are offered, Mail7 sends a responder SA that contains the IPSEC parameters selected; "Triple DES", "MD5," and "Public Key Original Mode." This completed, both sides know the IPSEC options that will be used for the connection.

Note: There are additional IPSEC options that must be negotiated during the establishment of an ISAKMP SA including: "Group description, type, prime, generator(s), curve(s), order, field size, life type, life duration, and PRF, but would entail more detail then necessary to discuss (Frankel, 91)."

4. After Frank01 obtains a certificate for Mail7 (either through direct communication with Mail7 or through the use of a certificate repository) he sends a nonce ("A nonce is a randomly generated value that is used to provide proof of liveliness and prevent replay attacks" (Frankel, pg. 96).), his own certificate, and the public portion of a Diffie-Hellman key exchange, all encrypted using the public key extracted from the certificate for Mail7.

5. Mail7 responds with his own certificate, a nonce, and his half of the public portion for a Diffie-Hellman exchange encrypted using Frank's public key (extracted from the Certificate provided by Frank01).

6. Now both parties have communicated the information needed to generate a Diffie-Hellman secret key. They do so, and then exchange an MD5 hash of the Diffie-Hellman secret key, the public portions of the Diffie-Hellman exchange sent by both sides, the Cookies (contained inside the ISAKMP headers) sent by both sides, the established Security Association for the connection, and their own Certificate.

7. At this point each side regenerates the corresponding hash and verifies the session has been successful in establishing a shared secret. An ISAKMP SA (phase 1 of an IPSEC connection establishment) is now complete.

8. Phase 2 begins with Frank01 using the established ISAKMP secured channel to send an IPSEC SA proposal message. This message contains similar data to the proposal sent for the ISAKMP SA in step 1. Included is a SA message (containing the various options for encryption, authentication, and protocol; AH or ESP), a Nonce (to prevent replay attacks), half of the public portion of a Diffie-Hellman exchange, and the Certificate of both Frank and Mail7.

9. Mail7 then responds with an encrypted packet, using the previously established ISAKMP SA, containing the same information, but only the options that it selected from those offered by Frank01.

10. Now both sides have the enough information to calculate, through the use of the Diffie-Hellman Algorithm, the keying material that will be used for the IPSEC SA. They do so, and Frank01 sends a final phase 2 message containing a hash payload of the message ID and the nonces from the first two messages. Once verified this confirms that an IPSEC SA has been established and secured IP communication can now take place over the channel.

By encrypting all transmissions between Frank's laptop and his e-mail server with IPSEC the data is kept Confidential (confidentiality), tamper free (integrity), and any services that require an IPSEC connection are ensured accessibility to only authorized users (availability).

Application Level Authentication

Now that a secured connection has been established the last thing that needs to take place before Frank can read his mail, is for Frank to authenticate himself to the Email Service on Mail7. Although authentication was required to establish a network connection to Mail7, the application itself, in this case Exchange 2000 running on Windows 2000 Server, will also require authentication. Windows 2000 uses Kerberos for Smart Card authentication. The following describes the

process that would take place according to the TechNet article referenced in the notes:

1. Frank01 sends Frank's certificate to the Key Distribution Center (KDC) *(aka Domain Controller).*

2. The KDC compares Frank's UPN (user principal name) in the certificate with the UPN on Frank's object in the directory. The KDC also verifies the signature on the certificate to ensure that it was issued by a Certificate Authority that is trusted by the Active Directory forest, in this case the Department of Licensing.

3. The KDC encrypts the logon session key and the Ticket Granting (TGT) for the Ticket Granting Service with the Public Key from Frank's certificate. This ensures that only Frank, with the appropriate private, key can decrypt the logon session key.

4. Frank decrypts the logon session key and presents the TGT to the ticket granting service, thus proving that the user is in fact Frank, through access to Frank's private key. Not only has Windows 2000 ensured that an authorized user is accessing Frank's mail box, Non-repudiation has been achieved since Frank's private key was used for the authentication, and Frank is the only one with that access.

Frank has now authenticated himself to his mail server to establish a connection thereby preventing the majority of availability attacks, established a secure connection that ensures both confidentiality and integrity, and established non-repudiation by using his private key. At no point in this scenario was Frank's use of wireless technologies a significant security threat.

Why not today?

There are several reasons that our network communications are not as secure as the picture painted above. One of the reasons we are still rarely using encryption is the performance hit associated with encrypting data.

> IP security *(IPSEC)* provides encryption of outgoing IP packets, but at the cost of local computer performance. On a computer with IP encryption enabled, packets are encrypted before being passed to the network, which is a processor-intensive procedure. Although IPSEC implements symmetric encryption of network data, encryption of a large amount of IP packets can tax all but the fastest workstations" (Windows 2000

Resource Kit).

This is especially an issue when encrypting all traffic, including non-sensitive data. Fortunately newer Public Key Algorithms, such as Elliptic Curve Cryptography, are being developed that will drastically reduce this performance degradation. Also network cards such as the one offered from 3com at www.3com.com provide for IPSEC processing in hardware ensuring performance degradation is prevented entirely.

Another problem is getting everyone to agree on standards. IPSEC is an Internet standard protocol that provides all the authentication and encryption discussed above. The problem is that unless everyone is using it, requiring your system only to communicate securely means that your system won't be communicating much at all, as the vast majority of systems are not employing it. Currently most web servers that need to provide secured connections employ SSL, an application level encryption that must be properly implemented by each application individually.

Lastly an economical, fully trusted Third Party has yet to appear on the scene. The most trusted 3rd party we currently rely on, VeriSign has greatly hurt the community's confidence by issuing certificates without properly verifying identity. As one example consider Microsoft Security Bulletin MS01-017 released in mid March where VeriSign issued a certificate to a hacker claiming to be a Microsoft employee, allowing him to, among other things, digitally sign software. In addition to "mistakes" such as this there is also significant costs associated with personal certificates. Currently a class 1 personal certificate costs $14.95 per year through VeriSign (verisign.com). For a 1000 employee company this can be a significant cost.

What to do today?

Since a globally deployed and trusted PKI won't be a reality for some time we must look at the world as it is today:

- Today SSL is used for the majority of online transactions and other sensitive information that traverses the Internet.
- IPSEC is generally used only for VPN connections, and servers that are considered extra sensitive on the LAN. This means that far and away the majority of data transmitted on our local area networks is insecure.
- Because physical security is not an option with a wireless LAN we must, at a minimum, deploy encryption to these segments.

The only way to mitigate the weaknesses exposed by our wireless networks is

to attempt to limit logical access, Layer 2 and above, to our insecure LANs. This means deploying a security gateway between the wired and wireless networks to limit access and encrypt data.

The most common form of a security gateway is a Virtual Private Network (VPN). VPN solutions are divided into two main categories, IPSEC and non-IPSEC. Non-IPSEC VPNs use solutions such as Microsoft's Point to Point Tunneling Protocol (PPTP) or other vendor specific solutions for encryption. With these solutions the bottom line is that unless the algorithm has been examined by the whole of the security community it will be insecure. This has proven true for non-IPSEC VPN solutions. If the need is VPN, IPSEC is the solution. An added benefit to using a security gateway is the ability to provide access control to the Internet. This is useful for preventing hackers from stealing Internet bandwidth. It is also an excellent way for service providers to charge for wireless Internet access.

A new security gateway technology that has been developed in response to the open physical layer of wireless networks is 802.1x. The low level details of 802.1x are outside the scope of this paper, but the concept is essentially that of turning each wireless access point into a security gateway that provides both authentication and encryption services before allowing access to the wired LAN. Unfortunately, researchers at the University of Maryland proved that 802.1x is vulnerable to man-in-the-middle attacks and session hijacking attacks that IPSEC was designed to overcome (Ephraim).

Conclusion

Wireless LAN technology such as 802.11b is a powerful advancement in network that greatly extends the physical boundaries of a LAN. This extension of physical boundaries provides expanded access to both authorized and unauthorized users. Because existing technologies such as PKI and IPSEC are not fully deployed our LANs are incredibly insecure causing this expansion of access to be dangerous. As a result, a separation of the wireless LAN and the wired LAN is necessary. This separation can be accomplished through the use of a security gateway; the most effective being an IPSEC VPN.

Works Cited

CERT® Incident Note IN-2001-09. 6 Aug 2001.
URL: http://www.cert.org/incident_notes/IN-2001-09.html (11 Oct 2002).
Cole, Eric. Information Assurance Foundations. SANS, 2001.

Currier, Bob. "WEP: No weapon against hackers." 26 Feb 2002.
URL:
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2689916,00.html
(11 Oct 2002).

Edwards, Mark Joseph. "Think You're Safe from Sniffing?" 1 June 2002. URL:
http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=8878 (11 Oct 2002).

Ethereal. URL: http://www.ethereal.com (11 Oct 2002).

Flickenger, Rob. "Antenna on the cheap (er, chip)." 5 July 2002. URL:
http://www.oreillynet.com/cs/weblog/view/wlg/448 (11 Oct 2002).

Frankel, Sheila. Demystifying the IPSEC Puzzle. Norwood: Artech House, Inc, 2001. 90 – 120.

Harkens, D and Carrel, D. "RFC 2409." Nov 1998. URL:
http://www.ietf.org/rfc/rfc2409.txt (11 Oct 2002).

Huey, Benjamin. "Penetration Testing on 802.11b Networks." 24 Feb 2002.
URL: http://rr.sans.org/wireless/test_80211b.php (11 Oct 2002).

Information Security Glossary
URL: http://www.yourwindow.to/information-security/gl_confidentialityintegrityandavailabili.htm

Menezes, A., Van Oorschot, P., and Vanstone, S. Handbook of Applied Cryptography. CRC Press. 1996. URL: http://www.cacr.math.uwaterloo.ca/hac/about/chap1.pdf (11 Oct 2002).

Metcalf, Ed. "Data Integrity Assurance-The Foundation For Your Security Strategy." 6 Feb 2002. URL: http://www.tripwire.com/literature/newsletter/020602/020602-a.cfm (11 Oct 2002).

Poulsen, Kevin. "When Dreams Attack." 31 July 2002. URL: http://online.securityfocus.com/news/558 (11 Oct 2002).

Product Offerings, 3com. URL: http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=13&selcat=Wireless+Products&family=89 (11 Oct 2002).

Schwartz, Ephraim. "Researchers crack new wireless security spec." 14 Feb 2002. URL: http://www.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml (11 Oct 2002).

TechNet. "Microsoft Security Bulletin MS01-017." 22 Mar 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-017.asp (11 Oct 2002).

VeriSign http://www.verisign.com/products/class1/index.html

Windows 2000 Resource Kit. "TCP/IP in Windows 2000 Professional." URL: http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/prork/prcc_tcp_bsks.asp (11 Oct 2002).

Zeitler, Roland and Yang, Jung-Uh. "Smart Cards and the Windows 2000 PKI." Mar 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smrtcard/smrtcdcb/sec1/smartc03.asp (11 Oct 2002).