Wireless Security:

Can You Protect Your Data Without Wires?

White Paper

Andrew G. Hargreave, III
Geneer Corporation

February 2001

Introduction

The year 2000 saw security rise up the ladder of awareness in the minds everyone involved in any area of technology. Security in the normal computing environment was difficult to get ahead of, as there were almost daily reports of another hole found in an application or operating system. Like a gust of wind on a forest fire, security on the rapidly multiplying wireless devices that folks are carrying around is starting to become the burning issue on the minds of everyone planning to utilize these new devices.

Where do you get started? What should you be worried about? This white paper examines the prevalent issues regarding wireless security and where someone entering this space should be focusing their attention.

Overview

*e*TForecasts.com reported in February, 2001 that "the number of Internet users surpassed 400 million in 2000 and will continue to grow strongly in the next five years. Most of the growth is coming from Asia, Latin America and parts of Europe. By year-end 2005 the number of worldwide Internet users will nearly triple to 1.17B. An increasing portion of Internet users will be using wireless devices such as web-enabled phones and PDAs to go online."[1] That many users accessing corporate data on devices that can easily be left behind at the airport or stolen while sitting on a table somewhere has to give any responsible CEO/CIO/CTO the shivers.

The other area that needs to be secured is the transport of the data itself. Today, there's not that much data that needs to be secured. Most of the wireless traffic is short messages saying "Meeting time has changed!" or someone is checking on the latest price for their stock portfolio. But the future is rapidly approaching where users will want to trade their stocks online, purchase goods/services online, and perform other business related transactions. These transactions do need to be secured so that unauthorized individuals don't intercept them. In addition to transaction security, security measures must be available to prevent the transmission and proliferation of viruses in these new computing environments.

The devices you use and the network they're connected to will determine what measures you can take to secure the transmissions.

Where Are the Vulnerabilities?

In the "wired" internet, there is an end-to-end physical connection between the servers and the clients, and all the security (firewalls, certificates, SSL, etc.) is fairly well established. Wireless introduces some extra steps into the mix that also need to be secured. Figure 1 shows a typical wireless model.

[1] http://www.etforecasts.com/pr/pr201.htm

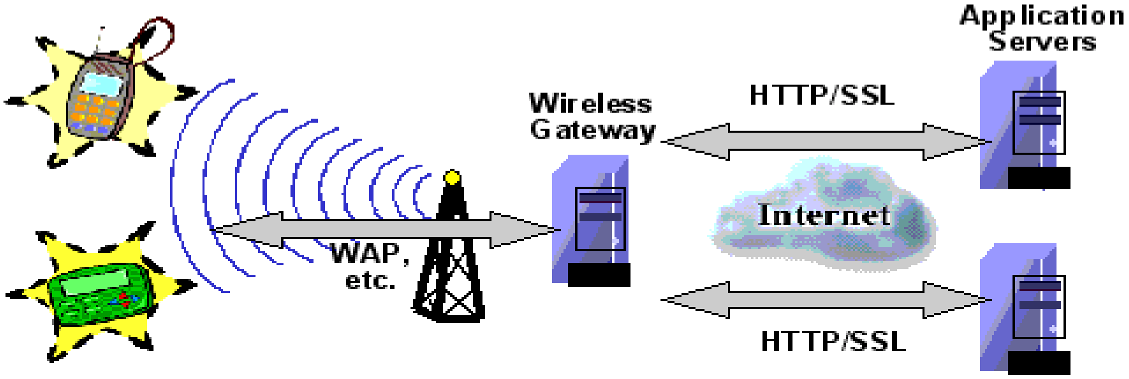

Figure 1: The Wireless Gateway Model[2]

In the wireless world, the data needs to pass through a gateway for translation into a format that can be recognized by the wireless network and the client devices. So the gateway needs to be secured, just like any other server. The next area to be concerned about is someone ”sniffing” the data as it travels though the air. The last links in the chain are the devices themselves. Each type device has its own unique processing power, operating memory, storage memory, and user interface that make developing one standard next to impossible. These characteristics also make it difficult to prevent infections by viruses or other malicious code.

Old Solutions to New Problems

Many of the prevailing and emerging solutions to the challenge of wireless security are based on or borrow heavily from the established solutions for wired network security. As we'll see, many common wired network security technologies have an analog in the wireless world.

Just as we told you back in our original Wireless White Paper[3], there are at the present several wireless worlds out there. So we’ll examine how security solutions map into each of these.

Security Takes Two Forms

As a preface for the discussion that follows, let’s review some of the basics of what we mean when we say "security".

When considering a conversation between two parties, it is secure when all of the following are true:

1. The sender is who they say they are.
2. The receiver is who they say they are.
3. The sender's message is receivable only by the intended recipient.
4. The sender's message is received in the exact same form as it was sent.

[2] https://www.verisign.com/rsc/wp/wap/wireless.html
[3] http://www.geneer.com/whitepapers/download.asp?filename=wireless

There are specific types of security mechanisms to address each of the above concerns. Respectively, they are:

1. Sender's Digital Certificate.
2. Receiver's Digital Certificate.
3. Transport Encryption.
4. Message's Authentication.

Digital Certificates are more or less the modern day equivalent of the paper-based world's notarized documents. A trusted third party, called a Certificate Authority, issues a digital certificate to a person or system (such as a web server) when sufficient evidence (and payment) has been supplied attesting to the fact that the person or system is who they say they are.

Transport Encryption is a means of ensuring that if anyone other than the sender or receiver views the message while it is being transmitted, it will not be meaningful. Typically, in the Public Key Infrastructure (PKI) arrangement, the sender's digital certificate becomes the basis for an encryption key that is used to encode the message. The recipient can then decode the incoming message using the sender's public key information, because they've already acquired the sender's digital certificate.

Message Authentication is a means to allow a receiver to verify that the message has not been changed while it was being transmitted. This is accomplished by including a compressed summary of the original message (called a ”hash”) with the message. The receiver can recalculate the hash of the message they received and check to ensure that it matches the hash of the message that was sent.

Not all applications demand all the aspects of security to be enforced, so historically, security mechanisms have been developed with a mix and match approach in mind. Increasingly however, the general public's expectation is that all of these aspects are enforced for any transaction that is purported to be secure.

Security Using Wireless Application Protocol (WAP)

Wireless Application Protocol is the granddaddy of protocols as it has been around a long time, is popular, and is targeted to support the majority of Internet-enabled cell phones and most PDAs on the market today. WAP specifications are being developed by the WAP Forum, a consortium of wireless handset manufacturers, service providers, infrastructure providers, and software developers.[4]

Over the air data security for WAP transmissions is achieved via Wireless Transport Layer Security (WTLS). Like its cousin in the wired realm, Secure Sockets Layer (SSL), WTLS digital certificates are used to authenticate a server (a Wireless Gateway) to a client (a wireless handset device). In the WAP 1.2 specification, WTLS has been extended to allow clients to authenticate to a server rather than a gateway. Note, however, that most WAP-enabled phones in use today use WAP version 1.1.

[4] http://www.wapforum.org

Although WTLS employs a design pattern similar to SSL, it actually implements a different digital certificate specification, called a mini-certificate. Mini-certificates are optimized for receipt and processing by typically resource-limited wireless handset devices.

While on the surface, it sounds like things are in pretty good shape here, they could be better. Unfortunately, because of the nature of the wireless-to-wired network transition and protocol conversions that occur on the Wireless Gateway server, there is a potential weak link in the system. For a few milliseconds, sensitive information resides in clear-text in the gateway server's memory when the hand-off from SSL to WTSL takes place. This means that, for the time being at least, the business relationship between the network operator and the content provider is key to ensuring end-to-end data security. A remedy for this situation is in the offing with the "Tunneling WTLS" specification, which eliminates the need for a protocol translation. Tunneling WTLS is part of the WAP 1.3 specification, due sometime in 2001.

Another promising feature that was added in WAP 1.2 is Wireless Identity Modules (WIMs). Basically this allows for a smart card to be the source of client certificate credentials. Future phones and PDAs would accept these WIMs and then take on the identity of the cardholder.

Security Using i-mode

NTT DoCoMo's proprietary, but standards-based WAP alternative, i-mode, enjoys widespread use in Japan.With the recent business relationship formed between NTT and AT&T, the odds look good that it may emerge in the US as a strong competitor to WAP.

Because i-mode is proprietary, very little is published about the details of how security is accomplished with it. The only area where any definitive statements have been made is with regard to the over-the-air portion of the i-mode network, where NTT DoCoMo attests that radio link between i-mode handsets and the cellular base stations uses proprietary protocols and encoding. Skeptics argue that since so little evidence has been presented that it is secure, one must assume it is not. For mission-critical or trade secret data, you may wish to steer clear of i-mode until such concerns have been quelled.

Now, on the other side of the coin, there are those who say that since NTT is one of the premier members of the WAP Forum, it's reasonable to assume that i-mode models itself closely after WAP in area of transport security. We expect the details to make themselves more clearly available when and if i-mode expands to the US.

Security with Bluetooth

Bluetooth, the personal area networking wireless protocol, doesn't have a very reassuring security story.

Bluetooth’s primary response to the issue of security deals only with trying to ensure that a message is received by only the intended recipient. Bluetooth accomplishes this via a technique called frequency hopping. The standard calls for two Bluetooth devices, while engaged in a dialogue, to make 1600 radio frequency hops per second, and to adjust their transmission power to a level just barely adequate to accommodate the proximity of the devices. These measures, originally developed to deal with interference on the radio band Bluetooth uses, also make Bluetooth transmissions difficult to eavesdrop upon.

Official sources say Bluetooth has "sufficient encryption and authentication" for home and business use. Bluetooth lives in the realm of both the network hardware and network transport, so it deals with the concept of "authentication" as being sure that two given devices are indeed supposed to be exchanging data with one another. As such, Bluetooth devices are authenticated to one another during a configuration operation performed by a user, on both of the devices they wish to "hookup" to each other. Every Bluetooth device has its own unique "Unit Key". When two devices are configured to talk to each other, a "Combination Key" and an "Encryption Key" are generated on each device for that connection. The Bluetooth specification allows for encryption key length negotiation, which implies that some devices will be more secure than others.

Overall, it seems Bluetooth has the basics covered and appears to be walking the line between capabilities and constraints. Its supporters argue that since its broadcast range is so limited, and since the data typically exchanged in these network conversations is likely to be extremely atomic, security measures beyond those provided within the specification should not be needed. Lets hope we never have to try telling this to the owner of some future Bluetooth enabled automobile who just had his car "hot wireless-ed" and stolen.

Security with Java 2 Platform, Micro Edition (J2ME)

Sun has defined three editions of the Java 2 Platform: Micro (J2ME^{TM}), Standard (J2SE^{TM}), and Enterprise (J2EE^{TM}). Micro Java is targeted to small devices from smart cards and cell phones to PDAs and set-top boxes.

While other technologies maintain security in the data exchanged between two remote processes, Java maintains security *within* a process. For example, suppose a handheld device was using WAP to transmit a credit card number to a sales site. As we've already discussed above, WAP's WTLS will protect the data as it travels between the two, but what’s to stop a malicious program, executing on the handheld device itself, from grabbing the credit card number as it resides in the handheld’s memory?

With Java, each program runs in a secure “sandbox” maintained by the Java Virtual Machine. Programs may be prevented from accessing each other’s memory, storage space and other resources.

In addition to Java’s built-in run-time security, a Java device may have access to standard libraries of security functionality. Classes such as **java.security.interfaces.RSAPublicKey** and **java.security.acl.NotOwnerException** are available in the Standard and Enterprise editions, and also in any Micro edition that chooses to provide them.

One further comment regarding the place of J2ME relative to WAP, i-mode and Bluetooth: There are Java standard libraries, packaged in what is known as the

Connection-limited Device Configuration (CLDC)[5] which provide J2ME applications with access to data delivered to the device via any of these means.[6] In general, Java provides a much more mature and comprehensive security system that will only be equaled by the other platforms with lots more development.

Conclusion

We're in the Wild West phase of the prospecting of the Wireless Frontier. Your best defense is a good offense. Identify market leaders and drive their products by demanding the security and data integrity your mission critical applications require.

As always, the security of your application should be appropriate to the sensitivity of the data and the amount of threat. After all, we don't put bank vault doors on the fronts of our houses, because we know bank robbers rob banks because that's where the money is. Construct worst case scenarios for your proposed wireless applications. If the worst thing that could happen, for example, is that a random email could be decoded with extreme effort, then your security measures may not need to be very stringent. If, on the other hand, perpetrators could penetrate your enterprise and steal or destroy sensitive information, then you may need to rethink the whole idea of using today's wireless technology.

Until J2ME or WAP1.2 comes into widespread use, security conscious enterprises will not introduce mission-critical, mission-sensitive wireless applications. However, if the current trend toward using common IP-based connectivity for cell phones accelerates, and the computing ability of the devices increases, you may soon be able to use the very same security protocols you now use on the Internet with wireless devices.

It's as we always say: If you're not terrified about security, you're not paying attention!™

Links

WAP Forum
http://www.wapforum.org/

i-mode Faq
http://www.eurotechnology.com/imode/

Bluetooth
http://www.bluetooth.com/

Java 2 Platform, Micro Edition
http://java.sun.com/j2me/

SUN MICROSYSTEMS' JAVA[tm] TECHNOLOGY POWERS NTT DOCOMO'S NEW MOBILE INTERNET SERVICES
http://www.sun.com/smi/Press/sunflash/2001-01/sunflash.20010130.1.html

[5] http://developer.java.sun.com/developer/technicalArticles/wireless/midpapi/
[6] http://www.sun.com/smi/Press/sunflash/2001-01/sunflash.20010130.1.html

ABOUT GENEER

Established in 1984, Geneer is a leading professional services firm specializing in the design and development of custom software applications. With a strong track record in using emerging software technologies to make its clients competitive in their market place, Geneer's longevity, dependability, and thorough understanding of technology and software development have earned it the honor of working for an outstanding group of clients, including many of the Fortune 100. Geneer was recently named as the first Microsoft Gold Certified Partner for eCommerce Solutions in the U.S.

GENEER EXECUTIVE BRIEFING SERIES

Geneer's Executive Briefing Series delivers essential insights on the future of e-business, the Internet, and the technology that can have a significant impact on your product and service offerings. If you are interested in receiving future Geneer white papers, please contact Geneer Business Development: 800-4-Geneer or 847-294-0300. For more information about Geneer, visit our web site at www.geneer.com or e-mail us at info@geneer.com.

"If You're Not Terrified About Security, You're Not Paying Attention"™ is a trademark of Stratvantage Consulting, LLC; used by permission.