Global Information Assurance Certification Paper

Submitted by:
Stephen H. Gillilan
Sr. Auditor-Sprint
stephen.h.gillilan@mail.sprint.com

Vulnerabilities within the Wireless Application Protocol

Overview

Just when some security professionals thought they were starting to get a handle on wireline security and its continuously evolving attacks from creative hackers and saboteurs, the world decides to go wireless. Informationweek predicts that the number of wireless device purchases will rise dramatically in the very near term, from 100M in 2000 to 220M in 2005. (1) Wireless transmission devices, which include cellular phones, personal data assistants, and pagers, utilizing either radio frequency or infrared transmission, are set to create a whole new challenges, as each scrambles for marketshare, functionality and to extend the corporate information infrastructure out to the mobile individual. Security professionals often struggle with physical security of their network elements inside the building; now imagine a frightening number of terminals walking around in airports and restaurants. Throw into this mix a new protocol stack, and indeed it is whole new security arena to master. Welcome to the world of WAP, the Wireless Application Protocol.

What is WAP?

In the early stages of the wireless web, it was enough to be connected to the Internet, maybe get directions or check a football score. Each day, however, new announcements are made on how to increase the productivity of the individual by bringing the corporate information literally to the palm of his hand. My own company's wireless division, Sprint PCS, issues new public announcements almost daily about extending the enterprise, allowing access to mission critical applications like PeopleSoft, Lotus Notes and Microsoft Exchange. (2) The need to stay in constant touch through email and even access corporate applications is critical. WAP, the Wireless Application Protocol, is an array of protocols and tools that that applies the application programming model of the Internet to mobile phones and PDAs. (3) WAP is a "specification for a set of communication protocol to standardize the way wireless devices can be used for Internet access, including e-mail, the World Wide Web, newsgroups...conceived by four companies: Ericsson, Motorola, Nokia, and Unwired Planet (which is now Phone.com)." (4) These specifications were intended to, and have in many ways, become the established standard by which handheld devices communicate with the Internet. (5)

The WAP Model

WAP presents four primary attributes: an Internet programming model; a wireless markup language; an optimized protocol stack for wireless networks; a de facto standard supported by wireless device OEMs. (1) The diagram below sets forth a comparison between the Internet and WAP application programming model (1):

	Internet	WAP
Content Development	HTML JavaScript	WML WMLscript
Web Application Delivery	HTTP	Wireless Session Protocol Wireless Transaction Protocol
Secure Connectivity Protocol	TLS SSL	Wireless Transport Layer Security
Basic Transport Protocol	TCP/IP UDP/IP	Wireless Diagram Protocol Bearer Network: SMS, CDPD, CDMA, GSM, TDMA, etc

Submitted by:
Stephen H. Gillilan
Sr. Auditor-Sprint
stephen.h.gillilan@mail.sprint.com

Given the population of wireless users is rising quickly, and the access they are being granted to critical systems through the Wireless Application Protocol, it is important to understand the WAP model, and in particular, its security component, the Wireless Transport Layer Security (WTLS).

WTLS

WTLS is a hybrid creation, much of it scripted out of the specifications of Transport Layer Security (TLS), and some attributes from the Secure Socket Layer, (SSL), both of which allow a decent level of comfort and safety within internet connections and transactions. (6) WTLS was devised in large part because when it comes to handheld devices, accommodations must be made for the wireless network and the handheld device. In terms of the wireless network, it is less robust than wireline networks—less bandwidth, connection stability, and reliable availability, more latency. (3) Factor that with a handheld device with a limited CPU and memory, varied input devices, and restricted power consumption (3), and it makes some sense that the old Internet model might not work. In sum, WTLS is supposed provide privacy, data integrity, and authentication for applications on handheld devices. (6) However, changes made within WTLS to accommodate wireless devises have left it vulnerable to several security problems. (6)

Vulnerabilities

Critic Markku Juhai Saarinen has discovered a number of vulnerabilities within the WTLS (6):

- ***"Predictable IVs lead to chosen-plaintext attacks against low-entropy secrets."*** The WTLS protocol's internal structure requires that packet information carry decipherable information, in essence, an "oracle" which provides information concerning the users chosen password, allowing the password to be cracked by bruteforce with a relatively small amount of data captured from that user. (6)
- ***"The XOR MAC and stream ciphers."*** WTLS supports specific MACs (Media Access Controller) which do not ensure data integrity and is particularly weak when used in conjunction with stream ciphers. (6)
- ***"35-bit DES encryption."*** Early versions of WTLS utilize inadequate levels of encryption, in particular 40-bit DES encryption. (6)
- ***"The PKCS #1 attack."*** RSA PKCS # 1, version 1.5, if used within WTLS for signatures and encryption has been shown to vulnerable to decryption if packet data reveals the RSA version. Some error messages in WTLS may provide this packet data. (6)
- ***"Unauthenticated alert messages."*** Alert messages within WTLS may be sent in cleartext, and may lack proper authentication. These messages can be substituted by an attacker for a valid datagram without the endusers knowledge, essentially destroying the data integrity of the message. (6)
- ***"Plaintext leaks."*** Packet level data information can be derived from initial connection messages and sequence numbers, allowing a hacker to derive intelligence concerning the type of encryption employed by the user. (6)

Submitted by:
Stephen H. Gillilan
Sr. Auditor-Sprint
stephen.h.gillilan@mail.sprint.com

There are other, less arcane issues that must be coped with by WTLS. For one, as an enduser connects between his device and the company server, the WTLS session stops, and the TLS session begins—essentially creating a void as the encryption of the message starts and then is restarted. (1). A second issue to consider is the use of digital certificates. At the present time, mobile phones have neither the storage nor processing power to handle encryption efficiently. One study by the phone manufacturer, Ericsson revealed that phones took up to 15 minutes to negotiate the RSA handshake process for WTLS connections. (1).

Are there alternatives?
One real question is why put up with another protocol stack and uncertain security concerns at all? The limitations of the wireless network and its handheld devices may quickly go away, particularly if the customer demands it. Storage capability and processing power are most likely not far off in the wireless world, and a seamless integration with corporate networks would appear to make some sense. A small but vocal group called the Free Protocol Foundation describes the Wireless Application protocol as a flawed standard and technical failure (5). In reality, WAP is here to stay-- LotusNotes has stated that their product line "will move toward WAP as the market does." (2) WTLS should harden and improve.

Steps to Take
First off, security professionals need to understand the differences and assurances provided by SSL, TLS and WTLS as enterprise applications and networks extend from the wireline LAN to a mobile environment. WTLS cannot be taken for granted if the vendor or mobile carrier states that their application incorporates it. The WAP stack was set out not by the broader Internet community as TLS and SSL were, but by several specific vendors looking to organize the wireless business space themselves. Which is fine, but if you are depending on WTLS to ensure security for remote connectivity to your corporate LAN, it is necessary to be cognizant of its inherent structure and weaknesses. Be aware of the improvements pending in the protocol. The lack of assurance provide by the first versions of WTLS is already being address by vendors with beefed up WTLS versions which support a higher level of encryption—up to 128-bit—and more efficient processing. (For example WTLS Plus by Certicom) Next, and maybe most importantly, stop thinking of cell phones and PDAs as personal property of employees, and start to view them as a corporate laptop remotely accessing the network.. Those measures which are in place to address that risk space should be organized and vigorously applied to business units allowing individuals to access mission critical applications.

Submitted by:
Stephen H. Gillilan
Sr. Auditor-Sprint
stephen.h.gillilan@mail.sprint.com

References:

1) Levitt, Jason. "Web Apps take the Airwaves." June 26th, 2000. www.informationweek.com/792/wap.htm
2) Ross, Patrick Ross. "Sprint PCS Targets Business Customers." August 23rd, 2000. http://news.cnet.com/news/0-1004-200-2592819.html
3) "WAP: Wireless Internet Today." Wireless Application Protocol White Paper, June 2000. http://www.wapforum.org/what/whitepapers.htm
4) WAP. August 16th, 2000 www.whatis.com
5) Banan, Mosen. "The WAP Trap: An Expose of the Wireless Application Protocol." May 26th, 2000. http://www.freeprotocols.org/wapTrap/one/main.html
6) Saarinen, Markku-Juhani. "Attacks against the WAP WTLS Protocol." University of Jyväskylä, 1999.