Global Information Assurance Certification Paper

Security Models for M-Commerce
Joseph (Ted) Combs

Abstract

Electronic commerce or e-commerce has exploded since the commercialization of the Internet. For the quarter ending September 30, 2000, Commerce Department figures indicate a 15.3% increase over the previous quarter and total online retail sales of $6.4 billion. With overall retail sales of $812 billion for the quarter, online sales still represent less than 1% of total retail sales. (4) The huge online retail market and the obvious market potential exist, at least in part, due to the trust consumers have in online transactions. The security provided by online merchants including Secure Sockets Layer (SSL) and digital certificates enable this trust.

With the projection of 530 million wireless subscribers by the year 2001 and over one billion by 2004, attention has turned to mobile commerce (m-commerce). (6) M-commerce is defined as "the buying and selling of goods and services through wireless handheld devices such as cellular telephones and personal digital assistants." M-commerce, also known as next-generation e-commerce, gives consumers access to the Internet while they are away from their PC or Laptop. (5)

There is wide speculation that m-commerce will surpass wire-line e-commerce as the method of choice for online commerce transactions. In order for this to happen, the content delivery over wireless devices must become faster, more secure and scalable. M-commerce includes financial services such as mobile banking and brokerage services; telecommunications account management, bill presentation and payment; service and retail orders and payments; and information services including news, sports and traffic updates. (5)

The enabling technology behind m-commerce is the Wireless Application Protocol (WAP). WAP is the de-facto standard for the presentation and delivery of information and telephony services on wireless phones and terminals. The WAP Forum founded in 1997 by Ericsson, Motorola, Nokia and Phone.com developed the Wireless Application Protocol. The forum now has over 400 members. (6)

Security to enable the wireless Internet is defined by the Wireless Transport Layer Security (WTLS) specification. WAP version 1.1 includes the WTLS specification and was approved by the WAP forum in June 1999. According to Phone.com, "WTLS is poised to do for the wireless Internet what SSL did for the Internet – open whole new markets to e-commerce opportunities." (7)

Present Security Model

The WAP version 1.1 specification and WTLS provide the current model for security of m-commerce. WTLS, which provides for confidentiality, integrity and authentication, is

the wireless version of the Transport Layer Security (TLS) standard. TLS was derived from Secure Sockets Layer (SSL) 3.1. TLS, which provides a secure connection between a client browser and a server, is "too weighty" a protocol to use with the limited processor power, memory and battery power of the current handheld wireless devices and the high latency, low bandwidth environment. WTLS provides an optimized handshake through dynamic key refreshing and enabling more data compression than TLS. The dynamic key refreshing allows the encryption or session keys to be updated on a regular or configurable basis. (6,7)

The WAP security model has three components. The first part from the wireless device to the WAP gateway uses WTLS to secure the information sent over the wireless network. The second part, the communication over the Internet is secured by TLS (SSL) from the WAP gateway to the web server. The third component is the WAP gateway, which acts as a bridge and client proxy for the TLS portion of the communication and translates between WTLS and TLS. (7)

For high value, m-commerce transactions the use of the WAP gateway creates security concerns. The so-called "gap in WAP" is the momentary translation between WTLS and TLS, which for a few milliseconds allows the information to reside in clear-text in the server's memory. Because of this vulnerability, additional compensating layers of security are needed to protect the WAP gateway when used for high-risk transactions. Some of these protections include:

1. Ensuring the gateway never stores decrypted data to secondary storage media.
2. Use a translation process that is designed for security and speed so clear-text content is erased from internal memory as quickly as possible.
3. Provide physical security to ensure that only authorized administrators have access to the gateway and console.
4. Restrict the gateway from remote administrative access.
5. Apply appropriate hardening guidelines to the gateway server operating system. (7)

Although there is disagreement over the seriousness of the "gap in WAP," banks and financial institutions may accept the current security model temporary, but they will certainly drive toward end-to-end encryption of financial transactions over wireless networks. Some analysts take a serious view of the WAP gateway vulnerability. According to the Gartner Group 'enterprises wireless-enabling their operations leave themselves in "a state of constant risk" due to taking security shortcuts with emerging wireless devices and services.' (2) Certainly, "the current WAP security model requires a strong relationship between the network operator and the content provider to implement the most secure solutions possible." (7)

Future Security Models

The WAP Forum recognizes that a more flexible and extensible solution is needed for highly secure applications. These secure applications require that the content remain

encrypted from the time it leaves the application server until it arrives at the wireless handset and visa versa. End-to-end security using WTLS "tunneling" is included with WAP version 1.3 and is due sometime in 2001. This version of WAP will also allow for the reference of digital certificates. (7)

Interim solutions that improve the security of the information transmitted but fall short of end-to-end encryption includes installing a WAP Gateway server at the content provider or in the enterprise. (7) WAP version 1.2, when fully implemented, allows the gateway server to be placed at a content provider's premise, such as a bank, which is more secure than at the network provider's premises. (1,3)

Several vendors offer public-key infrastructure (PKI) products for use with mobile applications. Use of these PKI products allow wireless users to provide encryption, authentication and non-repudiation for wireless data. Especially important for high value transactions, the PKI allows the application provider and the user to authenticate to each other and to provide non-repudiation capabilities. (1)

WAP may turn out to be a temporary solution as advances in technology may eventually eliminate the need for a special, lightweight, protocol. Processing power, memory, battery and bandwidth limitations will be overcome and allow the use of standard Internet protocols. (1) Although the future of m-commerce security models and protocols is uncertain, today, WAP and WTLS are the main players for wireless transactions.

Works Cited

1. DeJesus, Edmond X. "Locking Down the Wavelengths." Information Security. Oct. 2000. URL: http://www.infosecuritymag.com/oct2000/locking.htm (7 Dec. 2000).

2. "Gartner: WAP Servers Are 'Hacker Magnets'." epaynew.com. 2 Nov. 2000. URL: http://www.epaynews.com (10 Nov. 2000).

3. Hablin, Matt. "Security Getting Better, Isn't a Barrier, Analyst Says." Computerworld. 17 Jul. 2000. URL: http://www.computerworld.com (30 Nov. 2000).

4. Kontzer, Tony. "Online Sales Look Good, But Key Questions Unanswered." InformationWeek Online. 27 Nov. 2000. URL: http://www.informationweek.com/story/IWK20001127S0004 (5 Dec. 2000).

5. "M-commerce." whatis?com. 4 Dec. 2000. URL: http://whatis.techtarget.com/WhatIs_Search_Results_Exact/1,282033,,00.html?query=m-commerce (4 Dec. 2000).

6. "Telepathy WST Whitepaper." Baltimore. URL: http://www.baltimore.com/library/whitepapers/wsecure.html (20 Nov. 2000).

7. “Understanding Security on the Wireless Internet.” phone.com. Jan. 2000. URL: http://www.phone.com/pub/Security_WP.pdf (4 Dec. 2000).

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor