Defining the security required for WAP based Mobile ticket sales

Alex Pandelidis
University of Ontario Institute of Technology
(UOIT), Canada
Faculty of Business and Information
Technology
2000 Simcoe Street North, Oshawa, Ontario
L1H 7K4
905-922-9578

Alex.pandelidis@gmail.com

ABSTRACT
M-commerce has not really been used to its full potential as of yet. With the advent of more powerful cell phones and PDAs entering the market there is an opportunity for more innovative marketing techniques to come into play. Currently to perform any kind of commerce in the mobile environment, users are required to use the WAP system to communicate with the internet. However the WAP system presents its own problems because there is a sever lack of security due to the nature of the operations. These issues are perhaps what have prevented mobile commerce from becoming a realistic solution. In the future there is promise of new technologies will address some of the security issues that have been presented within a WAP based mobile commerce system.

Categories and Subject Descriptors
C.2.6[**Internetworking**]: *Standards (e.g., TCP/IP)*

General Terms
Standardization, Documentation, Theory

Keywords
WAP, Security, Mobile Ticket Sales, and Cellular

1. INTRODUCTION
It has been said that the full ability of m-commerce has yet to be utilized. Throughout the dot com burst and the early 2000s, there has been little growth in the field that had promised so much. However more recently there has been a growth in the m-commerce sector, partially due to new applications that are being developed, one of which that will be discussed in this paper is that of mobile ticket purchasing.

PST 2006, Oct 30-Nov 1, 2006, Markham, Ontario, Canada

It is predicted that the year 2010 the business of mobile ticket sales will generate revenues in the area of $63 billion dollars, clearly this is a major industry that deserves a great deal of attention. [3] In theory M-Commerce would allow people to conduct business that they would normally be forced to do at home anywhere in the world; it would also allow companies to use location based strategies when dealing with customers. This theory could easily hold true for the issue of ticket sales, whether it's to sporting events, concerts, or other events. This would allow users to be free from their desktops and laptops (which require a more permanent type of connection either from home or an internet café) and be able to make purchases and transactions anywhere they wish. [1] A common example of the benefit of offering ticket sales to the mobile community is the ability of purchasing on the fly. Say that a person is planning on attending a club of some sort where there is a requirement for tickets to be purchased prior to the event. It is likely that the person would still be unaware of the specifics of the event on route to the location, using an m-commerce interface (cell phone, PDA, etc) would allow the user to purchase their ticket easily without having to actually go to the location where the event is being held. [1] Here is an example, say your heading into the city to visit some friends and enjoy a night out on the town. You have no idea what you want to do yet as your heading in on the train, however you do see several advertisements for various shows and concerts on the wall of the train, or perhaps you receive a text message from a friend of a show that is taking place. You pull out your mobile (PDA or cell phone) surf on over to your ticket purchasing agent site (TicketMaster or other) make the purchase on your phone, and your ready to go for the night. This is one example of how mobile ticket purchasing could be applied. Then at the event there would require some sort of identification to show proof of purchase, this paper however will not analyze that section of the transaction, rather the steps necessary to purchase the ticket through the users mobile. When dealing with this type of issue there are several technologies that come into play. First there is the mobile device itself which is too broad of a topic to be covered in depth in this article. Second there is the markup language, WML (wireless markup language which is XML being validated against a specified type of DTD document). Thirdly there is the WAP browser, also called the micro-browser which is a specialized designed browser that works on mobile phones and PDAs designed to view WAP pages (called "cards"). The last piece of technology that is relevant to this paper on the security aspects of mobile ticket purchasing is the WAP gateway [22]. The WAP gateway allows regular HTML pages found out on the Internet to be formatted into WAP documents that can be viewed

on mobile devices. The WAP gateway sits between the wireless network of the service provider (GSM or CDMA). If you refer to figure 1.1, you'll see that the WAP gateway is the wireless networks portal to the web, but also encodes the information so that it can be viewed on the web. Thus the scope of this paper will be that it will analyze some of the security risks that are present from the WAP gateway server to the client end (PDA or cell phone), but will not investigate any issues that are present on the application servers.

2. A brief explanation of WML and WAP

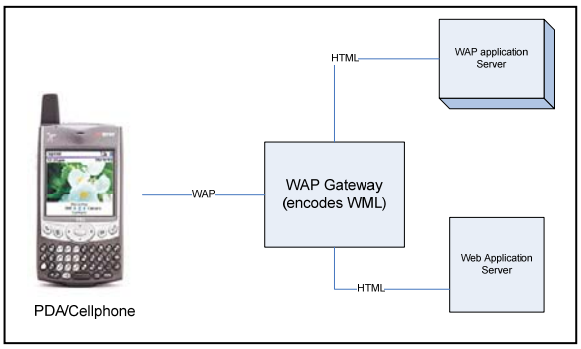
Before any kind of analysis can be done on the security of setting up a mobile ticket retail system, there must first be an understanding of what the primary technologies are that are currently being used in the mobile world. The current client server relationship that exists in the mobile world is defined by the standard called WAP, or wireless application protocol. Starting in 1998 WAP 1.0 was the first version that was used and provides the architecture to allow for mobile platforms.[1] This is necessary because of the restrictions of the mobile platforms, such as

- Small display
- Variations in the size and method of displaying information
- Text input is slower due to lack of real keyboard
- Not usually a mouse
- Currently only some providers have high speed access
- Users usually have to pay for each byte of data rather than time
- Lower processing power

[4] As you can see at current, there is a need still for a standard such as WAP 1.0 (and 1.1 or 1.2). The key to WAP 1.0 is that it uses what is called the "WAP gateway", as discussed above and shown in figure 1.1, the WAP gateway converts information that is transmitted in the standard format of the internet, HyperText Markup Language (HTML)/ HyperText Transfer Protocol (HTTP)/Internet Protocol (IP) to a WAP format, WML (wireless markup language). By doing this it allows websites and other web info to be sent in a more efficient way, so that they can be sent in Over the air transmissions (OTA) better. Although the WAP gateway maybe seen as merely a middleman in the equation simply used to convert information to WML format, there is more to it than that.

WML, a variant of XML is far less forgiving than other forms such as HTML[4]. WML is typical as most scripting languages.[7] Once the HTML file goes through he WAP gateway it becomes WML and any errors are removed, this again is a benefit to mobile devices because they won't have the processing power that their desktop counter parts would. In the future some have predicted that WAP 2.0 will become the standard. WAP 2.0 is a slim down version of XHTML, which would allow providers to drop the WAP gateway and eliminate that step. Some industry analyst have said that this will be the stepping stone to true HTML access on the mobile, and will allow mobile users to enjoy in full web pages, this however will not be discussed in this article.

Figure 1.1Showing the method of how WAP allows mobiles to connect to the Internet



3. How Mobile ticketing could work

Currently there are already a few areas where mobile ticketing exists, one example is in public transit. [1] The method that is frequently used currently is messages are sent through the SMS (short message service), this however is a less than perfect scenario. While SMS is a fairly universal and well implemented technology, it has its limitations for mobile ticketing. SMS is primarily text and does not have the best implementation for browsing of lists, as might be a list of events one wishes to purchase a ticket to. What is a more realistic option is browsing using a micro browser, which as discussed above would allow users to see WML formatted pages on their mobile that originally oriented on the regular internet.

4. Security issues with WAP/WML/SMS for Ticket Sales

Security is of vital importance to any m-commerce application (any commerce application actually). If the user does not have a sense of security it is unlikely that they will trust the seller they are doing business with and move on. There are five core issues of importance when discussing security issues with WAP/WML, they are: Authentication – making sure you are who you say you are, Confidentiality, integrity – ensure that the data gets to and from its destination unaltered or viewed, authorization, and non-repudiation – to ensure that once a party has voluntarily given information its not possible for them to deny giving any information. [5]

There are already measures in place to help deal with the issue of authentication, its called the wireless transport layer security protocol (WTSL). [5] WTSL works similar to TSL, in that it creates a session (referred to as a handshake between computers) between the two clients, which then can negotiate set parameters for protecting the session. The parameters dictated can include things like signature algorithms, public keys, pre-master secrets and exchange certificates. In the world of WTSL, the handshake is between the WAP gateway and the client (phone) so it would be up to the service provider (in Canada, Rogers, Fido, Telus, Bell, etc.) to chose which type of security they would like, and this would ultimately have an effect on whether companies who

do ticket sales (such as TicketMaster) would have an interest in hosting a service through cellular service providers.

Further, there are more security issues of trying to do commerce over a WAP connection, one of them is the gateway. The WAP gateway does the function (among many) of decrypting information that is sent via TSL (transport layer protocol) and converting it to WTSL, the wireless equivalent. [5] This is one area where there is a possibly security risk. Many would have you believe that this is not the case because typically the way that network providers have their services set up is such that they store the security keys in memory on their servers and supposedly the OS doesn't get a hold the keys. This represents a key flaw in the design of WAP, since all the information being sent from the users computer is being sent through this central server it leaves a lot of room open for unwanted people to get in to the vendors system. It is because of the trust that is built between the two systems in the "handshake" causes this problem. The information that is coming in TSL format must be decrypted and re-encrypted in WTSL format, thus for a short while that information is sitting unencrypted on the vendors machine [6]. This is a very unappealing idea for those who wish to make transactions over their phone, whether it's through their credit card or their SIM card.

Another security risk that is present with WAP technology is the encryption level that it uses; currently WAP only uses 35 bit encryption, which can be broken by hackers using "brute force" methods [6].

There are also physical security issues that become present with WAP when one is interested in creating an environment to purchase tickets via mobile. The method of identification for GSM phone providers is a piece of technology called a SIM card. This SIM card identifies the phone on the network of the provider. Billing is also frequently done this way for items such as internet access, SMS messaging, phone calls, etc. With the ease of a SIM card being lost of stolen leaves the users account open to incorrect authentication because it is so easy for someone to steal someone else's card (and whole phone).[7] There are also risks of SIM card duplication, where individuals manage to duplicate SIM cards and can use an account on more than one phone at more than one time[5]. On CDMA networks the problem is similar, except they do not use SIM cards rather the phones identification number is used for authentication of the user for payment of services.

As mentioned above, one possible implementation of mobile ticketing services is to the Short Message Service (SMS) which is currently available on nearly all service providers. This would provide a simpler and far more limiting method of doing mobile ticket services. In Finland, the way that this system is currently implemented is customers text message a 4 digit number to a premium service number and in return they receive the ticket in the form of an SMS message [7]. This method is not without its security risks; those worth of mentioning are risks of spoofing, spamming and SMS viruses. Since the phone number that the user is sending their ticket request is being sent through a variety of different systems (cell phone system, ticket provider system, etc) at any place it could be intercepted and become a target for spamming or spoofing, as well as a virus. There have been examples where individuals have created viruses that if opened on the user's phone would copy a list of all their contacts and send it back to another location. Clearly these issues aren't as significant as the issues around the WAP architecture but important none the less. [8]

A final issue for security with WAP/WML is the "crypto package" that is included in the WML library. WML script includes a specific library function called "crypto package", this library contains a signing function that can be used when digital signatures are required, such as a ticket purchase [7]. The crypto package uses a common public key type infrastructure. This however is somewhat flawed in encrypting data, since the information on the WML library set is available to everyone on the net, it seems highly plausible that someone with malicious intent could create a method of retrieving others information if they had access to the necessary resources. Thus this represents a critical security flaw in the nature of the Wireless markup language.

5. Possible solutions to Security issues

Of the issues discussed in this paper, new technologies that are being developed or have been developed will bring opportunities to solve a great number of the problems listed in this paper. The issues that are the greatest of importance are those that revolve around the WAP gateway. This is where information is decoded and then re-encoded so that it can be formatted to a WAP device. This problem would be (or rather is, but is yet to be fully implemented) with WAP 2.0 which uses a more streamline version of XHTML, has the promise of eliminating the WAP gateway, which would eliminate several of the security issues present with it. By eliminating the WAP gateway it would eliminate the need to decrypt then re-encrypt information, thus reducing a significant security risk. This would also solve the problem of WAP 1.1 using such a low encryption method, if WAP 2.0 was made wider spread.

Some issues such as the physical security issues do not have simple answers, and further research has to be done on ways of preventing unwanted users from accessing ones device, current passwords have a limited success in that they require the user to turn them on.

6. Conclusion and Future Works

To conclude, mobile ticketing has been effective in several parts of the world already, but there hasn't been any sort of large scale implementation as of yet. This may be due to several limitations of the devices that are slowly being overcome; one of these limitations may be the restrictions of WAP. There are several security issues such problems with the WAP gateway and its method of decrypting and then re-encrypting data, there are problems with physical security (which are far more difficult to solve), there are issues with using the SMS system, and there are certain problems with the WML library. A lot of these problems have the potential to be solved with the release of WAP 2.0, however I believe this is merely a stepping stone to the next step.

As PDAs and cell phones become more powerful and have better user inputs they will make it possible to use new ways to connect to the internet. Eventually it is likely that phones will be powerful enough to view HTML pages in their raw form with editing only being done on the receiving end (phone end) to make the page easily visible to the user. This will make mobile ticketing a more realistic option for more people, as more complex

searching and authentication methods become available it will being the world of mobile ticketing to more and more people.

7. References:

[1]J.J. Wang, Z. Song, P. Lei, R.E. Sheriff. “Design and evaluation of M-commerce Applications,” 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.

[2 accounting]Manish Agrawal, Hemant Padmanabhan, Lokesh Pandey, H.R. Rao, Shambhu Upadhyaya. “A Conceptual Approach to Information Security in Financial Account Aggregation,” ICEC ’04 Sixth International Conference on Electronic Commerce.

[3] Michael Semrau and Achim Kraiss. “Mobile commerce for financial services -killer applications or dead end?”, SIGGROUP Bulletin April 2001/Vol 22, N

[4]Anne Kaikkonen, Virpi Roto. “Navigating in a Mobile XHTML Application,” CHI 2003, April 5–10, 2003, Ft. Lauderdale, Florida, USA.

[5]Gianluigi Me. “Security overview for m-payed virtual ticketing.” The 1 4m IEEE 2003 International Symposium on PersonalJndoor and Mobile Radio Communication Proceedings

[6]Niels Christian Juul, Niels Jørgensen. “ Security Issues in Mobile Commerce Using WAP,” 15th Bled Electronic Commerce Conference eReality: Constructing the eEconomy Bled, Slovenia, June 17 - 19, 2002

[7 (6 ticketing acceptance)]Niina Mallat, Matti Rossi, Virpi Kristiina Tuunainen, Anssi Öörni. “The Impact of Use Situation and Mobility on the Acceptance of Mobile Ticketing Services,” Proceedings of the 39th Hawaii International Conference on System Sciences – 2006

[8]Jason Crampton.” Applying Hierarchical and RoleBased
Access Control to XML Documents,” ACM Workshop on Secure Web Services, October 29, 2004, Fairfax VA,
USA.

[9]Jun-Zhao Sun, Douglas Howie, Antti Koivisto, Jaako Sauvola. “A Hierarchical Framework Modle of Mobile Security,” 2001 IEEE.

[10]Mikko Hyppönen. “WAP and Viruses – Can Your Mobile Phone Get Iinfected?” VIRUS BULLETIN CONFERENCE ©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England

[11]Francis Till. “E-commerce solutions NBR Special Review Who needs a wallet when there's a phone?; You do, but this could be the year m-commerce finally kicks off”. The National Business Review (New Zealand) March 10, 2006.

[12]Seth Fogie, Cyrus Peikari. “For Wireless Security, First Understand Wireless Programming,” Informit.com Feb 14 2003 [cited April 2, 2006] available from World Wide Web: http://www.informit.com/articles/article.asp?p=30938&seqNum=2

[13]“OboPay launches m-payments service in US,” Finextra.com. March 30, 2005 [cited April 2, 2006] available from World wide Web: http://www.finextra.com/fullstory.asp?id=15126

[14]Lexis Nexis Academic search “Sales using mobile phones to skyrocket,” UPI 2006 HAMPSHIRE, England, Jan. 25 [Cited April 2, 2006].

[15]W3C Schools. “Introduction to WAP”, W3C schools,” [Cited April 2, 2006] available on the World Wide Web: http://www.w3schools.com/wap/wap_intro.asp

[16]Ric Howell, “WAP Security.” Top XML [cited April 2, 2006] available on the World Wide Web: http://www.topxml.com/wap/articles/wap_security/default.asp

[17]Ted Wugofski, Dave Raggett. “Towards Convergence of WML, XHTML, and other W3C Technologies,” W3C Organization, 31st May 2000, [cited April 2, 2006]. Available on the World Wide Web: http://www.w3.org/2000/09/Papers/Wugofski.html

[18]Treo information: cool gadgets. [cited April 2, 2006] http://alteraxion.typepad.com/coolgadgets/T650Blazer1.jpg [Treo internet pic]

[19]Channelsource image library: Treo SMS [cited April 2, 2006] http://channelsource.palm.com/regac_images/chsrc/imageLibrary/pi31ty08rw04rtu.jpg [treo SMS pic]

[20]Dan Zrobok. “The Security Issues with WAP” March 26, 2001 [cited April 2, 2006] available on the World Wide Web: http://www.cas.mcmaster.ca/~wmfarmer/SE-4C03-01/papers/Zrobok-WAP.html

[21] Job de Haas. “Mobile security SMS& WAP”, Black hat briefs Las Vegas 2001.

[22]Chiaxa Biancheri, Jean-Christophe Pazzaglia, Gavino Paddeu. “EIHA?!? " deploying Web and WAP services
using XML technology” SIGMOD Record, Vol. 30, No. 1, March 2001.