WAP: Wireless Application Protocol

Nick Barnett

INFO 1023_7A Networking Essentials

Professor Gary Sparks

Metropolitan Community College

Abstract

As the importance of staying connected to the internet through mobile devices has grown, the need for supporting technologies has also grown. Wireless Application Protocol (WAP) is a collection of wireless protocols that allow the transfer and display of webpages through text-only, microbrowsing cell phones and personal digital assistants (PDAs). Although not as popular as it was in the 90s, WAP was once the prominent way to connect to webpages via mobile devices. The research in this paper will explain how WAP works, security issues associated with WAP, and the changes made within WAP for security and development purposes. This paper will conclude with an analysis of the future applicability of WAP in an expanding, mobile wireless market.

WAP: Wireless Application Protocol

While smartphones have taken over the cell phone market within the United States, many mobile phone users in other countries are still using older phones that don't have large touch screens, full browser support, or high powered processors. In the late 90s, mobile phone users didn't have the option of purchasing smartphones, but still needed access to webpages. Wireless Application Protocol (WAP) was a solution that offered simplified versions of webpages for text only mobile phone screens. Although WAP doesn't seem practical for many Americans who surf the web through their mobile smartphones daily, "outside the US, roughly 80% of mobile phone users are still using WAP to browse the web" (Sarrel, 2010). Due to the exponential increases in technology that happen every year and that "designers have to create Web pages that adhere to strict guidelines in order for them to work with WAP" (Miastkowski, 2000), WAP may go the way of the dinosaur, but is still applicable with many devices around the world. This paper discusses the WAP model, how the protocol functions, and the applicability in past and future markets by addressing the following questions:

1. How does WAP work?
2. How secure is WAP?
3. What are the implications of WAP in an expanding wireless market?

Although smartphones utilize different protocols for mobile data transfer, WAP is still thriving with many users and the importance of the WAP protocol stack is still inherent with mobile web browsers delivering wireless content.

How Does WAP Work?

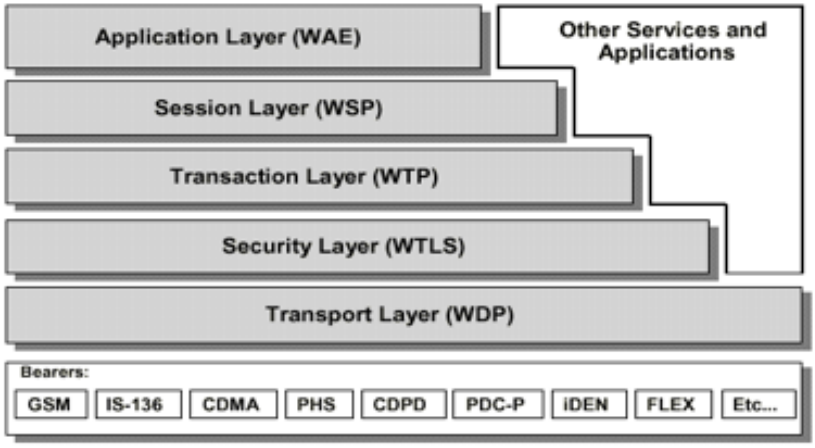
WAP is not a singular protocol, but rather a group of protocols, commonly referred to as a stack that loosely resembles the Open System Interconnection (OSI) model. In the 90s, more and more mobile users required access to webpages while on the go, so in "1997, Nokia, Motorola, Ericsson and Phone.com came together to create the WAP because they believed that a universal standard is critical to the successful implementation of wireless Internet" (Tyson, n.d.). The WAP stack includes Wireless Session Protocol (WSP), Wireless Transport Protocol (WTP), Wireless Transport Layer Security (WTLS), Wireless Datagram Protocol (WDP), and the Wireless Application Environment (WAE). In an online article *How it Works: Wireless Application Protocol,* PCWorld contributor, Stan Miastkowski, explains

> While you only notice the WAE part of WAP, the other parts play essential roles in the background. The Wireless Session Protocol establishes and closes connections with WAP Web sites. The Wireless Transport Protocol helps make sure data packets get where they're going. Wireless connections are less reliable than wired connections, so it's vital to make sure data that you send and receive are accepted. The Wireless Layer Security, a subset of the Secure Sockets Layer often used for credit-card-based transactions on the Web, compresses and encrypts the data sent from your wireless device (2000).

Much like the application layer of the OSI model, the WAE offers developers the use of Wireless Markup Language (WML) and WMLScript rather than the traditional combination of Hypertext Markup Language (HTML) and JavaScript which use "more memory and processing power to support a browser than is desirable for a wireless device like a cell phone or PDA" (Mitchell, n.d.). At the session layer, WSP establishes connections similarly to Hypertext Transfer Protocol

(HTTP), however, instead of using text data, WSP is able to transfer data more efficiently using compressed binary data.

Wireless Application Protocol



Note. Adapted from http://www.brainwareknowledgehub.com/content/?p=1049, 2011

WTP then follows at the transaction layer, performing similar functions to Transmission Control Protocol (TCP), but requiring less information be sent for each transaction. By performing TCP functions such as preventing duplicate packets being sent and retransmitting packets if needed, while lessening the information overhead attached to TCP, WTP is able to offer the same service over a mobile connection. At the security layer, WTLS provides encryption and authentication services before moving to the transport layer where WDP works with network carriers which use Internet Protocol (IP) or Point to Point Protocol (PPP) to provide an interface for information exchange between the network carriers and higher level protocols. The network carriers, or bearers, support Short Message Service (SMS) and General Packet Radio System (GPRS) for data transfer as well.

Due to older phones text-only limited displays, WAP accesses webpages with a microbrowser. The information requested transfers to a gateway server that gathers the information through HTTP. Since WAP uses WML rather than HTML, a WAP gateway server "includes the WAP encoder, script compiler and protocol adapters to convert the HTTP information to WML" (Tyson, n.d.). Once the information has been converted to WML, it is able to be viewed through the phones microbrowser.

How Secure is WAP?

With the involvement of WAP gateways comes possible security risks. Although WAP uses WTLS for encryption and authentication, when information is passed to the gateway to translate HTML to WML, "data is momentarily present in plaintext and it is this 'gap' in security that can, potentially, pose a serious security risk [and] may still be too unacceptable for services that require secure transactions, such as banking and brokerage" (SANS, 2001). These associated risks brought about a new version of WAP, titled WAP 2.0, which offers support for internet protocols such as TCP/IP and HTTP, negating the need for WAP gateways and providing secure end-to-end encryption and authentication. WAP 2.0 also upgraded from WML to Extensible Hypertext Markup Language – Mobile Profile (XHTML-MP) and started using Cascading Style Sheets (CSS) in order to reduce "development costs, allowing developers to write applications for both PC and WAP clients, using a common subset of language elements and development tools" (WAP 2.0, 2001). Even though improvements have been made in WAP 2.0, there are still vulnerabilities within security including the lack of a public key infrastructure (PKI) and lack of certificate authentication.

What are the Implications of WAP in an Expanding Wireless Market?

Since WAP was developed in 1997, mobile technology has grown by leaps and bounds. The rise of the smartphone and the wireless tablet computer have changed the way many think about mobile connectivity and how business can expand with remote access through the use of wireless connectivity products. In the United States of America, it is difficult to walk down many streets without seeing someone surfing the web on their mobile device, but "while the percentage of smartphone users in the developing world is growing, it's going to be three to five years before they are adopted by the majority of users" (Sarrel, 2010). Like many technologies, WAP was built for a specific need, and as the technology surrounding text-only, microbrowsing phones has changed dramatically, so will the need for WAP.

The advancement of data interconnection through wide area networks (WANs) and the digital communications riding atop of these has become truly astonishing in this day and age. The creation and use of WAP to bridge the gap between cell phone users and those who need regular access to webpages and real time information was revolutionary, but as time goes by, different technologies will revolutionize the industry. Consumers will continue to drive the direction of mobile technology, and less will be willing to invest in mobile technologies that don't offer full browser support. Although WAP was critical to the growth of mobile web browsing, Community for Information Technology Leaders author, Matt Sarrel, isn't far off when he states: "While WAP is not as dead as I previously thought, it still does have one foot in the grave and another on a banana peel" (2010).

References

Miastkowski, S. (2000, July 3). How it Works: Wireless Application Protocol. Retrieved October 25, 2013, from http://www.pcworld.com/article/17437/article.html

Mitchell, B. (n.d.). Introduction to WAP. Retrieved October 31, 2013, from http://compnetworking.about.com/od/wirelesswap/l/aa123000b.htm

SANS Institute. (2001). *SANS Institute white paper on Wireless Application Protocol 2.0 Security* [White Paper]. Retrieved from http://www.sans.org/reading-room/whitepapers/wireless/wireless-application-protocol-20-security-159?show=wireless-application-protocol-20-security-159&cat=wireless

Sarrel, M. (2010, May 28). The Mobile Web: What to do with WAP in 2010. Retrieved October 28, 2013, from http://www.cioupdate.com/trends/article.php/3884961/ The-Mobile-Web-What-to-do-with-WAP-in-2010.htm

Tyson, J. (n.d.). How WAP Works. Retrieved October 30, 2013, from http://computer.howstuffworks.com/wireless-internet1.htm

WAP 2.0 Specifications. (2001, August 1). Retrieved October 30, 2013, from http://xml.coverpages.org/WAP20-Announce.html

Wireless Application Protocol [Chart]. (2011, December 6). Retrieved from http://www.brainwareknowledgehub.com/content/?p=1049