Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Wireless Application Protocol (WAP): "What is it all about....How does it work"

This document is written as Introduction to the Wireless Application Protocol and as a high level view of where the industry is headed in respect to this particular protocol. The Wireless Application Protocol (WAP) is used primarily for handheld devices. By definition according to "Planning for PKI" by Russ Housley, WAP "is an open global specification for providing Internet communications and advanced service to mobile users with wireless devices." The industry sees the WAP protocol as being a comprehensive and scalea...

Copyright SANS Institute
Author Retains Full Rights

AD

WIRELESS APPLICATION PROTOCOL (WAP)

"What is it all about….How does it work"

By:
Dwayne D. Paro
Version 1.2e

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

TABLE OF CONTENTS

1 Introduction 4
2 WAP Forum 4
2.1 Forum Goals 4
2.1.1 Bring Internet content and advanced data services to wireless devices 5
2.1.2 Create a standard wireless protocol that works on all wireless network technologies 5
2.1.3 Make content and applications scalable across a wide range of wireless networks 5
2.1.4 Work with and expand existing standards 5
2.2 Standardizing Bodies 5
2.3 Industry Specification 5
2.3.1 WAP programming model based on WWW programming model 5
2.3.2 Use of Wireless Markup Language (WML) which is derived from XML 6
2.3.3 Use of Micro browsers, similar to Web Browsers 6
2.3.4 Use of a lightweight protocol to minimize bandwidth use 6
2.3.5 Framework for Wireless Telephony Applications 6
3 Features of WAP 6
3.1 Interoperability 6
3.2 Scalability 6
3.3 Extensibility 6
3.4 Flexibility 6
3.5 Reusability 6
4 Benefits of WAP 7
4.1 Standard for linking mobile units to the Internet 7
4.2 Founded by major leaders in the industry 7
4.3 Forum continually growing in membership size 7
4.4 Way to rectify Mobile information services bad track record 7
4.5 Defines an acceptable functional user interface 7
4.6 Optimizes standard web protocols 7
4.7 Provides a secure wireless connection 7
4.8 Provides a way to implement new functionality 7
4.9 Adapts new standards for the Industry 8
5 Controversies Surrounding WAP 8
5.1 Less Bandwidth 8
5.2 Less Connection Stability 8
5.3 Less Predictable Availability 8
5.4 Push Operation is not specified 8
5.5 Lack of cookies for session management 8
5.6 Premature encryption endpoint, doesn't encrypt to the Gateway proxy server 8
5.7 Small downloadable unit size 8
5.8 Very few handsets support WAP 9
5.9 WAP Standard is incomplete 9

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

6 Architecture 9
7 WAP Applications 10
8 Future of WAP 11

© SANS Institute 2001, Author retains full rights

1 Introduction

This document is written as Introduction to the Wireless Application Protocol and as a high level view of where the industry is headed in respect to this particular protocol. The Wireless Application Protocol (WAP) is used primarily for handheld devices. By definition according to "Planning for PKI" by Russ Housley, WAP "is an open global specification for providing Internet communications and advanced service to mobile users with wireless devices." The industry sees the WAP protocol as being a comprehensive and scaleable protocol. WAP is not a protocol that works on its own. Rather WAP is designed to sit on top of other protocols to include; Code Division Multiple Access (CDMA) or Global Systems for Mobiles (GSM). WAP focuses on using existing standards and improving upon those to come up with a much more comprehensive solution. The wireless devices that are referenced in this document include but are not limited to the following:

- Mobile Telephones
- Pagers
- Personal Digital Assistants
- Other Wireless Terminals

WAP provides a way for businesses to produce new business opportunities. The technology is the same no matter what network platform is being used. Over the years there has been a considerable amount of work done to support desktop and larger computers. This technology can is needed because hand helds typically have the following limitations:

- Less Powerful PC's
- Less Memory
- Restricted Power Consumption
- Smaller Displays
- Different Input Devices

2 WAP Forum

The WAP forum was established in 1997 as a non-profit industry association. According to WAP Forum they define themselves as the following: "The Wireless Application Protocol Forum is an industry group dedicated to the goal of enabling sophisticated telephony and information services on handheld wireless devices." The original participants in developing WAP and the Forum were Motorola, Nokia, Ericsson and Phone.com. There are currently over 200 members.

2.1 Forum Goals

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2.1.1 Bring Internet content and advanced data services to wireless devices

The forum wanted to be able to design an ability that would allow users to be able to have access to resources regardless of location. Due to the fact that the user base for these products don't exist in a central location the ability to have access remotely for things such as email and internet access is paramount.

2.1.2 Create a standard wireless protocol that works on all wireless network technologies

In order for any technology to gain acceptance and continue to grow it must be standard. Therefore the forum recognized that the protocol that was to be developed had to be an open standard protocol that could be adopted and used by all vendors producing wireless products.

2.1.3 Make content and applications scalable across a wide range of wireless networks

Not all wireless networks want to provide exactly the same content and abilities. In order to be competitive the forum recognized that vendors would need the ability to scale what they intended to provide to the wireless community.

2.1.4 Work with and expand existing standards

It was recognized that there was no time to invent and new standard to operate and gauge wireless technology by. Therefore the forum decided that their specification would be based on improving existing standards and expanding on existing technology.

2.2 Standardizing Bodies

The forum works with several other standardizing bodies. These include but are not limited to:

- European Telecommunications Standards Institute (ETSI)
- Cellular Telecommunications Industry Association (CTIA)
- World Wide Web Consortium (W3C)
- Internet Engineering Task Force (IETF)

2.3 Industry Specification

The WAP forum has come up with an industry-accepted specification. The specification has five principal components:

2.3.1 WAP programming model based on WWW programming model

Using an existing standard programming model allowed for programmers to benefit from existing technology. The familiar programming model would allow developers to adapt to providing wireless technology solutions without having to learn a new model. This also allows the developers to continue to use existing development tools.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2.3.2 Use of Wireless Markup Language (WML) which is derived from XML

WML is very similar to XML with the exception of changes needed to make the language applicable to wireless. For example WML does not assume that a keyboard or mouse is present to enter data. Also it allows images to be displayed on very small screens.

2.3.3 Use of Micro browsers, similar to Web Browsers

This allows information to be presented to the user in a small and efficient manner. The similarity in the interface allows users to adapt to its use quickly.

2.3.4 Use of a lightweight protocol to minimize bandwidth use

Using a lightweight protocol stack allows the devices to use much less bandwidth making them more efficient.

2.3.5 Framework for Wireless Telephony Applications

This allows vendors to produce secure telephony applications that integrated with the WMLScript. Such a technology would be something like call forwarding.

3 Features of WAP

WAP has many key features that are representative of what the WAP Forum claims the protocol to be:

3.1 Interoperability

The key to WAP acceptance is that it operates as an open license free standard. This will allow vendors to use it with their wireless products and keep the technology growing.

3.2 Scalability

Works with many transport protocols and on a wide range of hand held devices so that a wider range of users can be reached regardless of what wireless device is being used.

3.3 Extensibility

As vendors produce newer and more various forms of wireless products the WAP must easily adapt to new technology to ensure continued usability

3.4 Flexibility

WAP must be able to work well with many applications requirements. This will allow many vendors to be able to play to the same tune when they are furthering the development of their products.

3.5 Reusability

Extends and adapts to existing Internet standards so that as the standard is further developed it can be added to and continue to grow.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4 Benefits of WAP

WAP is becoming a very hot topic in the industry. Many companies are in the process of developing specific WAP Divisions within their organizations for the following reasons:

4.1 Standard for linking mobile units to the Internet

There has never been an established standard for connection mobile units to the internet that could be used across all hand held devices. WAP will provide this in an efficient manner as it continues to grow and be developed.

4.2 Founded by major leaders in the industry

Many large leaders in the industry have started the WAP Forum and are staking their reputation on its success in becoming an industry standard.

4.3 Forum continually growing in membership size

Due to the various originating members of the forum other large companies are gradually joining the forum and adding to the success of the protocol.

4.4 Way to rectify Mobile information services bad track record

There have been many security issues related to wireless protocols. WAP is working on making sure that as the protocol evolves that these security risks are addressed.

4.5 Defines an acceptable functional user interface

Users must be able to easily adapt to an interface in order to be motivated to use it. Users prefer that regardless of which wireless product they choose that the interface will be similar across the board. That is why the WAP has decided to use a mini browser interface similar to a web browser interface.

4.6 Optimizes standard web protocols

WAP decided up front upon establishment of the forum that they wanted to build on existing technologies to further the industry rather than creating a whole new protocol. This appeals to developers because they don't have to learn a new model to work by.

4.7 Provides a secure wireless connection

Users are not only very concerned with the ability to view their email but to also be able to do this in a secure manner. If they don't feel they can do this then the technology is of no use to them. WAP forum has made secure connection a very important part of developing the standard.

4.8 Provides a way to implement new functionality

In working along the same lines as the open standard for development vendors want to provide the ability for new functionality to be added to their existing products. Added functionality is what helps sell the product to new and existing users.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4.9 Adapts new standards for the Industry

Not only does the WAP forum want to work from existing standards they also want to be able to contribute new standards that can be used throughout the industry. This shows that they are not just working off established technology but are also contributing new technology to the industry.

5 Controversies Surrounding WAP

As with any protocol or industry standard there exists limiting factors and proponents to the standard or technology. WAP is no different and has the following limitations:

5.1 Less Bandwidth

Due to the fact that wireless products use less bandwidth they are unable to transfer large amounts of data. This can be very restrictive in areas such as receiving email and responding to email.

5.2 Less Connection Stability

There is no guaranteed continued connection with the handheld wireless device. The server could drop connection during a transfer session without notice and the transfer would have to start over.

5.3 Less Predictable Availability

Not all networks natively support the wireless application protocol so availability of resources tends to be limited.

5.4 Push Operation is not specified

Not all handheld devices can support data being pushed to them. The handheld client is dependent on the standards the server uses to push the data.

5.5 Lack of cookies for session management

Not having cookies available for holding the session together, WAP uses indexes in URL instead. This is because many handhelds don't support cookies in HTTP header information.

5.6 Premature encryption endpoint, doesn't encrypt to the Gateway proxy server

This is due to the fact that the Handheld device doesn't have capability to talk directly to the Host. Protocol translation issues prevent the endpoint being the Host therefore it is the Gateway instead.

5.7 Small downloadable unit size

WAP doesn't yet support any form of compression. The WML is also limited to 1,400 bytes. Therefore the program has to be extremely code efficient, of which most are not.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

5.8 Very few handsets support WAP

Most handhelds to date do not support the use of WAP. This is primarily due to the lack of standardization and industry acceptance.

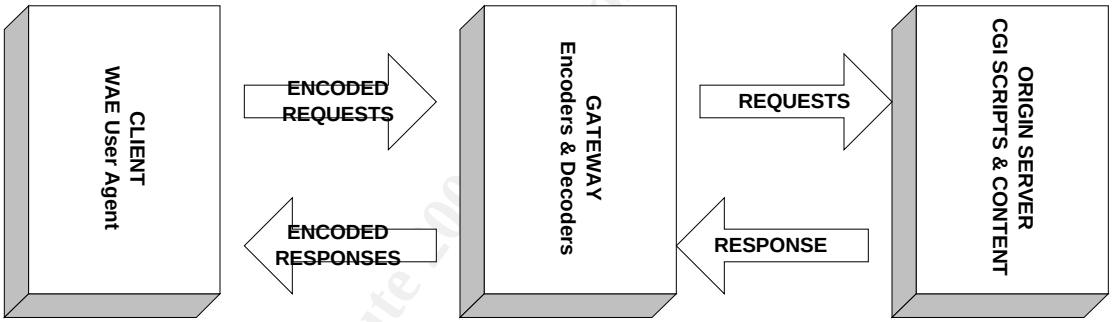
5.9 WAP Standard is incomplete

To date the WAP standard is still under improvement. There is no final standard that exists today meaning that as vendors develop their products to work with the protocol they could be forced to change things based on how WAP changes.

6 Architecture

The WAP model follows the OSI model very closely in its structure. The model uses five layers to include; Application, Session, Transaction, Security and Transport. WAP is more than a basic communications protocol. There are several architectural components that make up WAP.

- A microbrowser is installed into the wireless device. This requires very limited resources from the wireless device.
- A WAP gateway, which resides in the carriers network.
- A Web Server to host the WAP content.



The WAP gateway receives all requests coming in from the wireless devices. The Gateway translates these requests from WAP requests into HTTP requests. These requests are forwarded to the Web Server for processing. The Web Server then processes these requests and provides the information back to the wireless devices via the Gateway. The Gateway then takes these responses and translates them into binary WML files. Due to the protocols used for transport the WAP Gateway is a necessary component. The Gateway and wireless devices use a transport protocol that the Web Server can't understand. It translates the requests into a form, typically HTTP that the Web Server can understand.

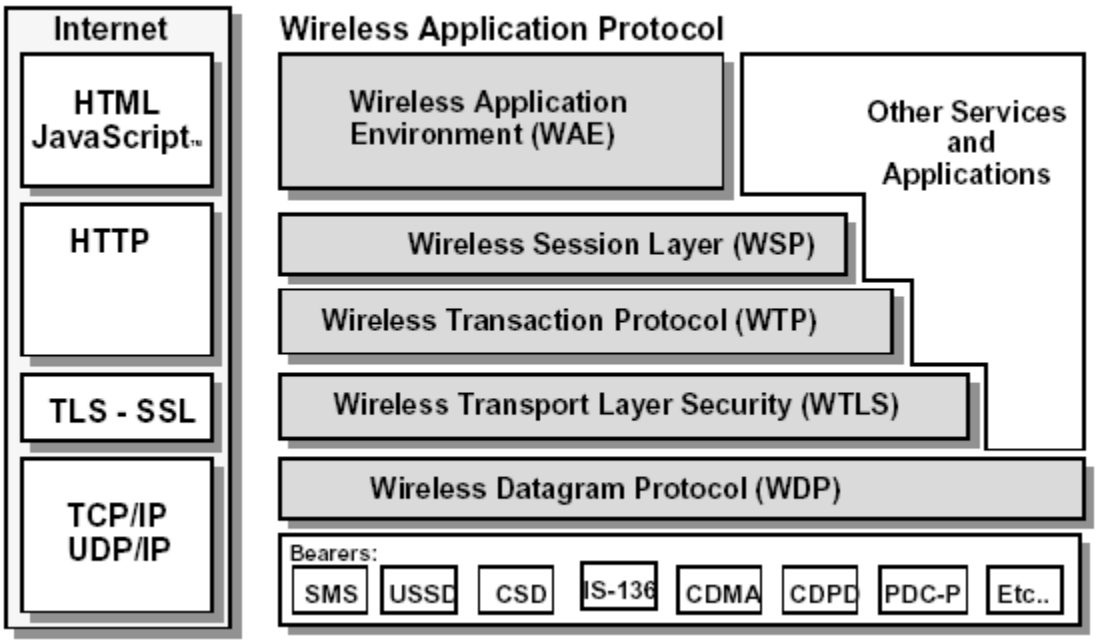
WAP Applications reside on the Web Server so no software has to be installed on the mobile device. Encryption and authentication are provided through Wireless Transport Layer Security (WTLS). This security is based on Transport Layer Security and SSL The encryption options are DES and 3DES.

The overall architecture of WAP is layered, which is represented below:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Wireless Application Environment (WAE)	User Interface on remote device
Wireless Session Protocol (WSP)	Links WAE to two session services
Wireless Transaction Protocol (WTP)	Runs on top of UDP
Wireless Transport Layer Security (WTLS)	Incorporates security features
Wireless Datagram Protocol (WDP	Bearer independent adapting to transport layer
Bearers e.i. Data, SMS, USSD	

According to Nokia Wireless Software Solutions the diagram below depicts WAP protocol architecture and a comparison to the Internet Protocols:



7 WAP Applications

WAP support is emerging in more and more existing mobile hardware and software suppliers products. These applications help to increase the productivity of employees allowing them to have continuous access to various resources.

Specific areas of applications that are being expanded to include the support of WAP are in the following:

- Person to Person Messaging
- Voice and Fax Mail Notifications
- Unified Messaging
- Internet Email
- Prepayment
- Ringtones
- Mobile Commerce

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Affinity Programs
- Mobile Banking
- Chat
- Information Services

The earliest forms of WAP applications were news feeds, stock quotes, and weather forecasts.

Example of wireless applications are Web Clipping and Advantgo. Each one is discussed below.

Web Clipping was designed for the Palm VII. This application delivers web content that is suitable for limited display. This could be things such as stock quotes, weather forecasts and such. Web Clipping uses the architecture defined above to include a client side application, proxy server and a web server. The client side of the software is Palm Query Application (PQA), which is a record database. The actual Web Clipping application resides on a web server and between the Palm and the web server is the proxy server to help facilitate the transfer of data.

Advantgo is very similar to Web Clippings with some distinct differences. Data is transferred between devices during a connected synchronization with the Palm and the web server. Advantgo's server has the ability to shrink images to make them viewable on a handheld device, getting rid of unusable content and compressing HTML. There is a client portion that goes on the Palm which includes a web browser and mini web server. The server and client sides are connected via Mobile Link.

8 Future of WAP

Depending on whom you consult with the future of WAP in general is not very clear. The industry has yet to take a stronghold on the idea and no one company has stepped up to become the founding leader in the technology. There is no doubt that the technology will remain and at some point will become a critical player in the industry. At this time there are several security concerns that prevent it from moving at the pace of the rest of the established industry. With the continued research and funding of large corporations the technology will make significant milestones.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

WORKS CITED

Mitchell, Bradley. "Introduction to WAP – WAP Applications." Http://compnetworking.about.com/library/weekly/aa123000c.htm

Mobile Lifestreams. "Yes 2 WAP – An Introduction to the Wireless Application Protocol." 1 April 2000. http://www.yes2wap.com

Open Market. "Open Market Solutions for Wireless Devices." 6 July 2000.

Nokia Wireless Software Solutions. "Wireless Application Protocol – The Corporate Perspective." March 1999. http://www.nokia.com/corporate.wap

Perkins, John. "WAP – What is it." October 2000. http://www.cimi.org/public_docs/r_wap.html

Mitchell, Bradley. "Introduction to WAP – What exactly is WAP." http://compnetworking.about.com/library/weekly/aa123000a.htm

"Wireless Application Protocol – White Paper." June 2000. http://www.wapforum.org

Housley, Russ. "Planning for PKI." January 2001. John Wiley and Sons Inc.

© SANS Institute 2001, Author retains full rights

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**