Global Information Assurance Certification Paper

Secure Wireless Application Protocol (WAP) in the Enterprise, Ready or Not?

Created By: Marcus L. Cutts

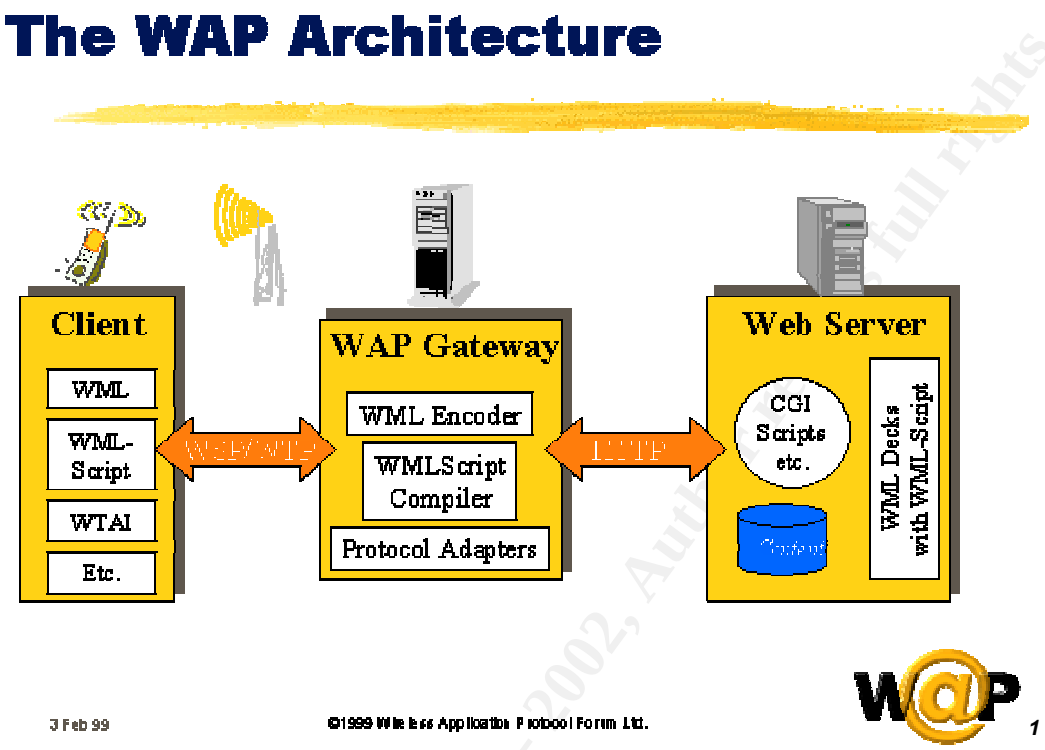
Abstract

The initial advent of wireless infrastructures and associated technologies were originally overlooked by most within the technological community. This was mostly due to the infantile nature of the technology, as well as its failure to address absolute critical issues such as security. Other variables such as cost and reliability also played a part in the shunning of wireless technology. However, the astounding acceptance and ingraining of the Internet into the everyday operations of life have spawned an overwhelming requirement and desire for access to unlimited amounts of information under virtually no restraints. We now find that being able to receive email and access calendar information among numerous other data only from the confines of ones office or home PC is not only unacceptable, but also a serious detriment to business and enterprises alike. Once again the endless possibilities of wireless communications and technology enters the stage, but this time it is unquestionably here to stay.

At the dawning of the 21st century we see an overwhelming interest in wireless technologies. This interest is not only for the luxuries and conveniences that they promise, but also for the sheer magnitude in which they can and probably will change the way in which enterprises are run and maintained in future generations. One such technology that has grabbed the communities', as well as the general public's attention is the Wireless Application Protocol (WAP). WAP is an open industry-established world standard that is based upon successful Internet standards such as, but not limited to the eXtensible Markup Language (XML) and the Internet Protocol (IP). By being established using already existing and accepted protocols WAP was destined to gain a tremendous amount of recognition from the start. However, regardless of the glitz and glamour the protocol still must meet certain requirements and be capable of certain functionality before it will be deemed suitable for the enterprise. One important issue, if not the most relevant of these requirements is the concern of adequate security within the technology. For, if the potential implementers of this protocol are not guaranteed secure communications and transactions all of the aforementioned glamour will be lost.

The intent of this thesis is to examine the WAP, and more specifically deal with security measures that have been included within the protocol. The document will provide an in-depth look at how this technology is structured and implemented, as well as how secure it is perceived throughout the industry within enterprise environments. Upon reviewing this paper the reader should develop an informed opinion on whether or not the WAP is ready for enterprise operations. That is not to conclude that more in-depth research should not be conducted, but is simply implying that the document could serve as an introduction and foundation of knowledge on the subject topic.

WAP Architecture

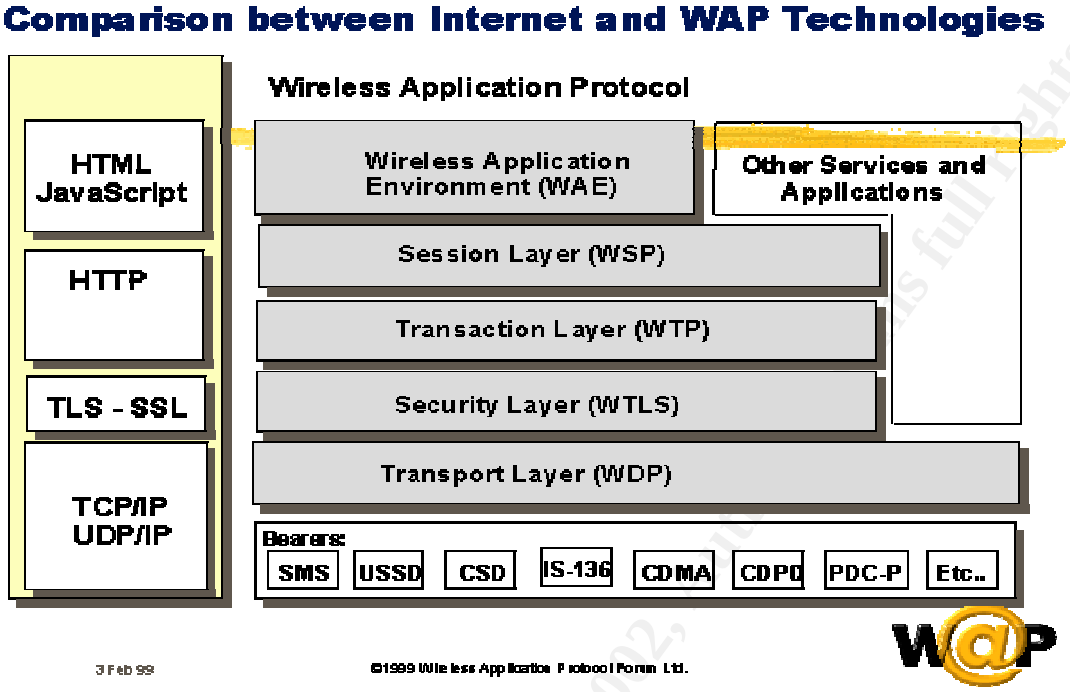


The image above depicts the architectural model of the WAP. It was designed to be extremely similar in nature to the existing protocols that make up the World Wide Web (WWW); this is further substantiated by the following comments that exist within the WAP architectural specification. "The WAP programming model is similar to the WWW programming model. This provides several benefits to the application developer community, including a familiar programming model, a proven architecture, and the ability to leverage existing tools (e.g., Web servers, XML tools, etc.). Optimizations and extensions have been made in order to match the characteristics of the wireless environment. Wherever possible, existing standards have been adopted or have been used as the starting point for the WAP technology."[2]

The components of the WAP architecture are illustrated in the image below. As one can see the protocol has taken into consideration the concerns of security from the beginning, this was not the case when wireless functions were initially introduced. However, although the creators of the WAP specification have addressed security, it is the industry consensus that the initial release of the protocol did not sufficiently cover security concerns and that it should definitely be given the utmost attention within subsequent releases. The image below shows how the subject protocol capitalizes on already existing, proven standards to achieve its end goals. Specifically, in the area of

[1] WAP Forum
[2] WAP Architecture Specification

security the Wireless Transport Layer Security (WTLS) component of the WAP architecture builds upon the industry standard Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to provide the necessary Bedrock Principles functionality.



Wireless Transport Layer Security (WTLS)

"WTLS is intended for use with the WAP transport protocols and has been optimized for use over narrow-band communication channels. WTLS provides the following features:

· Data integrity – WTLS contains facilities to ensure that data sent between the terminal and an application server is unchanged and uncorrupted.

· Privacy – WTLS contains facilities to ensures that data transmitted between the terminal and an application server is private and cannot be understood by any intermediate parties that may have intercepted the data stream.

· Authentication – WTLS contains facilities to establish the authenticity of the terminal and application server.

· Denial-of-service protection – WTLS contains facilities for detecting and rejecting data that is replayed or not successfully verified. WTLS makes many typical denial-of-service attacks harder to accomplish and protects the upper protocol layers. WTLS may also be used for secure communication between terminals, e.g., for authentication of electronic business card exchange. Applications are able to selectively enable or disable WTLS features depending on their security requirements and the characteristics of the underlying network (e.g., privacy may be disabled on networks already providing this service at a lower layer)."[2]

WTLS was created in order to facilitate secure wireless transactions without the need for extensive processing power and large sums of memory. WTLS promotes the fast processing of security algorithms. This is accomplished by reducing protocol

[2] WAP Architecture Specification

overhead and enabling increased data compression in comparison to that of traditional SSL solutions. The resulting effect is that WTLS can conduct appropriate security within a wireless network. These advances allow portable, wireless devices to communicate securely over the Internet.

"A secure WAP conversation occurs in two stages. First the transmission between the web server and the WAP gateway occurs over SSL. The onward transmission of this message over the air interface to and from the WAP browser device is over wireless networks using WTLS. Essentially the WAP gateway serves as a bridge between the WTLS and SSL security protocols. There are considerations (some say limitations) in the introduction of a bridging protocol like WTLS. The current WAP security model requires a strong relationship between the network operator and the content provider. The WAP Forum has recognized that as the market for highly secure applications increases, a more flexible and extensible solution will be needed. When working across many different wireless networks, application developers must be assured that their content remains encrypted from the time it leaves their application server until it arrives at the WAP handset. As a result there is a process underway to develop this more advanced security solution, which must address the enterprise's need for higher security and the operator's need for proper integration with WAP gateways in the wireless network."[3]

The previous paragraph, which provides an overview of a secure WAP conversation or transaction, describes the WAP gateway as a bridge between WTLS and SSL protocols. This gateway or bridge to many is also considered a possible security vulnerability to enterprises that utilize WAP based applications. The gateway is generally supplied by outside carriers who provide these capabilities externally to normal corporate operations. Thus, removing the assurance of secured operation from a portion of the WAP infrastructure. However, though these security concerns exist the WAP forum has diligently addressed such issues and has intent on easing these concerns in later releases of the WAP specification.

WTLS Certificates

In recent years one of the most effective and accepted ways of providing secure authentication has been through the usage of digital certificates. This has proven to be sufficient for hard-wired systems, and wireless equivalents are definitely not the exception. The wireless certificates have been produced and vigorously promoted by several independent vendors who actively support this technology as a means to provide wireless consumers with secure interactions, this is further substantiated by the following technical comments provided by Verisign.

From the security perspective, the most significant WAP specification is the Wireless Transport Layer Security (WTLS) protocol. WTLS is a close relative of SSL, the primary protocol used to secure the wired Web. For PKI, WTLS uses two types of certificates.

[3] Mobile Management

"**WTLS server certificates**, defined as part of WAP 1.1, are used to authenticate a WTLS server to a WTLS client (handset) and to provide a basis for establishing a key to encrypt a client-server session. They are like SSL server certificates, except that two different certificate formats are defined - X.509 certificates (as in SSL) and WTLS mini-certificates, which are functionally similar to X.509 but are smaller and simpler than X.509 to facilitate their processing in resource-constrained handsets. The mini-certificate is mandatory to implement and the X.509 certificate is optional to implement.

WTLS client certificates, defined as part of WAP 1.2, are used to authenticate a WTLS client (handset) to a WTLS server. They also can be formatted as either X.509 certificates or mini-certificates. WAP 1.2 also defines an interesting PKI-based function that is not part of WTLS. This function, which allows a WAP client to digitally sign a transaction, is known as the WML2 Script Sign Text function, and is intended for applications that require non-reputable signatures from clients."[4]

As stated earlier the initial release of the WAP specification was ridiculed due to its lack of consideration for security concerns. However, the WAP forum has meticulously progressed in the area of security and continues to make strides in providing secure wireless applications. This is evident in the ability provided in WAP 1.2 to handle wireless client authentication. With providing this functionality the WAP Forum has also made it possible for independent wireless security providers to expound upon the newest specification. This is further verified in the following comments.

"In a WAP environment, client-to-gateway authentication is provided within WTLS in WAP 1.2. Client-to-application authentication requires functions at a higher layer than WTLS. VeriSign favors an extension to the WAP WML Script standard to include a client authentication function akin to the Sign Text function. In essence, this function will work by having the client send to the server a digitally signed copy of a fresh challenge received from that server. The nature of PKI support for client authentication is essentially the same as for client digital signatures. X.509-format certificates are issued through VeriSign OnSite or related VeriSign service provider products, and are stored and used in the wired infrastructure and, optionally, in the client device or SIM."[4]

In addition to the aforementioned SIM, it is also evident that the industry is progressing in the area of wireless security, infrastructures, and applications simply by the onslaught of new standards, products, and concepts being introduced. One of these new innovations is the Wireless Public Key Infrastructure (WPKI), which will continue to aid in the progression of wireless efforts. The chart below provided by Baltimore Technologies demonstrates the promised capabilities of WPKI in comparison to SIM.

[4] Secure Wireless E-Commerce with PKI from VeriSign

	WPKI	SIM Toolkit
Approach	Infrastructure	Client Side
Model	Internet	Constrain Business Model
Focus	m-Commerce particpants	Operator centric
Availability	2001 (commercial)	Mid 2000
Overlap	SIM valuable but not essential	Can be integrated to WPKI
Standards	Agreed by WAP Forum	Implementation Specific
Market	Plan to use, Handsets committed	Tactical, Operator drive

[5]

Cryptographic Algorithms for Wireless Environments

Any adequate security solution must guarantee absolute confidentiality for its users, the most common way of achieving this requirement is through the use of encryption. Over the years many different algorithms have been introduced and utilized for encryption functions. One of the more prevalent cryptographic technologies has been the RSA crypto-system; this is especially true for the wired Internet environments. Although, RSA has proven to be an extremely valuable and reliable solution the question has often been posed, is there a better solution out there. To answer this question developers and integrators alike have begun extensive research into other potential encryption algorithms. One of the formidable competitors of RSA is Elliptic Curve Cryptography (ECC), which can perform the same basic functions as RSA but which demands fewer CPU resources and smaller data items that need to be communicated or stored.

Furthermore, the question is now frequently asked, which algorithm is more efficient for wireless environments? While all organizations must come to their own conclusion on the subject Verisign has chosen to take a path that will probably be less traveled. Verisign has chosen to implement both algorithms, this is illustrated in the following statements. "VeriSign possesses both RSA and ECC technologies and can apply either, as governed by market demand and service deployment costs."[4]

Verisign also makes it clear when the issue of selecting one of the two algorithms is absolutely necessary, and the associated determining factors involved in the following

[5] Comparison of WPKI and SIM Toolkit
[4] Secure Wireless E-Commerce with PKI from VeriSign

comments. "However, when considered in terms of the cryptography used in server key pairs and certificates (that is, the certificates processed by mobile clients), the question becomes moot. The RSA public-key operation, such as that used in verifying a digital signature, is no more resource intensive than the corresponding ECC operation. Consequently, given the extensive installed base of RSA technology, the industry appears to be embracing the use of RSA in this situation.

The question is more valid when considering cryptography for client authentication or digital signatures, because ECC private-key operations (such as digitally signing) can be much less resource-intensive than the corresponding RSA operations. However, the temptation to adopt ECC is countered by the fact that the installed base of Internet signature-verifying systems is RSA-based, hence leveragability of installed technology favors RSA. VeriSign's position is that RSA cryptography is preferred because of the foregoing factor, unless the platform is simply incapable of performing an RSA private-key operation in an acceptable time. In the latter case ECC is a good choice. Our experience to date has indicated that very few platforms have problems with RSA."[4]

The previous paragraphs are pretty convincing in stating that RSA's is the algorithm of choice within the Internet community, this is also proven by its enormous acceptance by corporations and standards bodies within the same industry. However, that is not to imply that the possibility of ECC gaining ground is not feasible. This is especially a consideration when one thinks about the opportunities and new technologies that will come to fruition in the years to come. Furthermore, events that are to soon take place may play a significant role in deciding how relevant new algorithms will be in the future. An example of such an event is the expiration of RSA's patent in the coming weeks. This may well be a leveraging point for other algorithms and encryption technologies, as the relinquishing of RSA's stronghold on the industry may very well be in trouble. Only time will tell!

Conclusion

The underlying question that this document presents is, if WAP is ready for extensive introduction into the mainstream of enterprise environments? The fact of the matter is that the answer is totally dependent upon the enterprise that is seeking the functionality that the WAP specification can provide. One question that organizations should first ask themselves before attempting to implement WAP functions is, are their infrastructures secure now; before the inclusion of wireless technologies? If the answer to this question is no, then those companies definitely have a greater concern that wireless capabilities.

The truth be told WAP is an extraordinary revelation for the industry, and especially for the opportunities that exist for wireless communications. However, the fact still remains that the protocol is but a babe, and in its infancy there still exists some

[4] Secure Wireless E-Commerce with PKI from VeriSign

areas that need improvement. It is also evident that the WAP Forum, as well as the community that it serves also realizes this and has been working vigorously to address these issues.

There is no doubt that WAP will play an important role within enterprises that desire its functions, the true task will be in corporations properly selecting appropriate areas to securely apply this technology. A suggestion to potential users is to first implement an exhaustive pilot program to test the performance and functionality within their specific enterprise. Furthermore, it is probably even more important to guarantee that the security measures provided by WAP are sufficient for their intended programs. Finally, it is my opinion that although the technology may be well on its way to being ready for prime time it is currently not there yet. This is primarily due to the continuing security concerns that exist around the standard, as well as the fact that it is still extremely new and has not been repeatedly proven within the industry. I do however expect this state to change rapidly, as major improvements and progressions are taking place in this area, and I for one am extremely excited about the possibilities, but for the time being I guess I will be left chomping at the bit!

Bibliography

1.) WAP Architecture, The WAP Forum,

http://www1.wapforum.org/member/developers/slides/WAP-Architecture/index.htm, 1999

2.) WAP Architecture Specification, The WAP Forum,

http://www1.wapforum.org/tech/terms.asp?doc=WAP-100-WAPArch-19980430-a.pdf, 2000

3.) Mobile Management, Market Drivers for the Foundation of The Open Group Mobile Management Forum, The Open Group, 2000

4.) Secure Wireless E-Commerce with PKI from VeriSign, Verisign Inc.,

https://www.verisign.com/server/rsc/wp/wap/index.html, 2000

5.) Comparison of WPKI and SIM Toolkit, Mobile Internet Security, Baltimore Technologies, 2000