What are some of the security concerns of WAP Does it have direct impact on the development of wireless smart devices?

Welcome to Brainstorm!

There are definite concerns over how secure WAP is as a technology and whether it is robust enough to implement applications with stringent security requirements.
Eustace Asanghanwa, Applications Engineering Manager, Atmel
Wireless Application Protocol (WAP) is an open standard technology that enables wireless smart devices, like mobile phones and PDAs, to access the Internet through network technologies like the mobile phone GSM and CDMA. With WAP, people can use their smart devices to perform activities such as email, purchase tickets and download music and news headlines.

Smart devices are not capable of directly handling content-rich Internet traffic. Unlike desktop and laptop computers, smart devices have lower communications and processing bandwidth, and smaller memory capacity. For this reason, they rely on WAP gateways to translate between the Internet's Hypertext Transfer Protocol (HTTP) and equivalent, but modest content and less resource-intensive combination of Wireless Session and Transaction Protocols (WSP and WTP). For security, WAP offers Wireless Transport Layer Security (WTLS) as optimized equivalent to the Transport Layer Security (TLS) of the Internet.?

The application infrastructure and physical limitations of smart devices present serious security vulnerabilities with WAP. First, end-to-end security is not possible between device and Web servers. In order to translate, the WAP gateway must decrypt all traffic, which momentarily renders content vulnerable. Add applications like banking and stock trading into the mix and it is only a matter of time before gateways come under heavy attacks.

In addition, device limitation in memory capacity and processing power forces usage of rudimentary cryptographic algorithms highly susceptible to hacking. Even worse, support for cryptography is optional, thus opening yet another vulnerability between device and gateway. A bank server, for example, would authenticate and deliver encrypted content to the WAP gateway only for the WAP gateway to decrypt and send the content in plain text to the smart device without the knowledge of the bank.

A possible solution to these vulnerabilities is to pull in the WAP gateway within a trusted perimeter, but this is less practical and brings about a different set of issues. Effective solutions will directly impact the development of wireless smart devices. Including hardware cryptographic capabilities in the form of Trusted Platform Modules (TPM) and secure microcontrollers into the device lightens

application-processing burden thus allowing it to use stronger cryptographic algorithms. Taken one step further, the addition of hardware accelerators may eliminate the need for a gateway. In a market characterized by high pressures on price and miniaturization, these are expensive additions but the value of security in upcoming more sensitive applications will justify the cost to the consumer.
Jim Alfred, Director of Product Management, Certicom
WAP security originally used WTLS as a security protocol optimized for constrained devices –"turn of this century" mobile handsets. While WAP 2.0 with SSL/TLS support is now widely deployed on handsets with XHTML capable browsers, a large number of mass market handsets in some markets still use a WAP 1.2 compatible browser. Thus the security of WAP is a relevant question. Given the bad reputation that WAP security initially received, it is worth re-examining.

The good part of WAP is the comprehensive client and server security support. This enables secure, efficient exchange of symmetric session keys, and anonymous and authenticated encryption of data, including signed messages using digital certificates and strong, efficient Elliptic Curve Cryptography, or ECC. Options for WAP security include anonymous key exchange, certificate-based server authentication and mutual authentication using both client and server certificates. WAP 1.2 added the ability to manage cryptographic keys and sensitive device information via the SIM card, making devices themselves more secure.?

The "bad" of WAP WTLS security is two-fold. Firstly, while WTLS does support authentication, the WTLS specification allows devices to specify weak encryption algorithms, including 40-bit DES, and predictable initialization vectors. Secondly, the "WAP Gap" in WTLS created a significant amount of bad press. WTLS security terminates at the WAP gateway, typically controlled by the service provider and acts as a proxy between targeted web servers and the mobile device. The gateway is left to secure the connection to the web site using a separate SSL/TLS connection, but data bridging the connection is in the clear. The notorious WAP Gap caused many to question whether mobile devices were suitable for sensitive applications or e-commerce. Even worse, because of the bad publicity, some did not implement WTLS at all.

With the advent of WAP 2.0, end-to-end security is supported via secure SSL/TLS tunnels directly between the handset and the web server, with no gateway interdiction. TLS provides for the same authentication schemes as WTLS, but without the gap. Problems with weak cryptography are also improved, with mandatory algorithm requirements and recommendations for their use.
?
What needs to happen now is for the industry to educate end users on the security features in WAP 1.2 and 2.0 handsets, and demand the appropriate levels of security in their clients and gateways. Doing this will instill confidence in the mobile Internet.

Source URL (retrieved on *09/16/2014 - 11:57pm*):
http://www.wirelessdesignmag.com/product-releases/2008/09/what-are-some-securi

ty-concerns-wap-does-it-have-direct-impact-development-wireless-smart-devices?qt-digital_editions=0