GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

John G. Schramm
12/2/00

Security Issues in WAP and I-Mode

WAP

Early this year (2000), the type of content available to wireless users was limited mainly to weather, news, sports, stock quotes, etc. The nature of this informational data did not require robust security measures, and the attainable level of security was not high enough for most banks and brokerage houses to offer their online services to wireless customers.

Although the WTLS specification within WAP provided strong security between a WAP client and the gateway, there was no way for WAP to interface directly with the Internet, and all WAP traffic had to be translated to HTTP in the gateway in order to reach content servers on the web. This became known as the Gap in WAP. Anything that was encrypted with wireless protocols had to be decrypted in the gateway then re-encrypted with Internet protocols, and vice versa.

To bridge this gap, the WAP Forum developed additional specifications, and now can offer the end-to-end security that will enable wireless e-business and banking.

Patrick Imbert of Gemplus identifies two functions that will be necessary to conduct banking and other commerce activities on the wireless network:

- the ability to exchange electronic documents
- the ability to make secure payment transactions.

In the first case, *" strong user authentication, integrity and confidentiality of the data exchanged and end-to-end security between the service provider and the end-user are key in the deployment of the service."*
In the second case, a *" non-repudiation mechanism for the payment transaction, acceptance of the security scheme by the banking organizations (VISA, Mastercard…), and again end-to-end security between the payment authority and the end-user are essential for the deployment of the service."*

The WTLS specification provides for 3 modes of operation:

- privacy and data integrity only
- privacy, data integrity and WAP gateway authentication
- privacy, data integrity, WAP gateway authentication and WAP client authentication

The similarity between WTLS and SSL/TLS is no coincidence, as WTLS was based on SSL 3.0 (TLS 1.0).

Most SSL implementations that we are familiar with on the Internet require server authentication to ensure end-users that they have not accidentally clicked their way to some rogue web site. Client authentication is generally accomplished via userid and

© SANS Institute 2000 - 2005 Author retains full rights.

password, and not by digital certificate. There are many reasons why the typical web user is not likely to have a certificate. Among them is the user's ability or inability to keep a private encryption key private.

Smartcards have long been proposed for holding digital certificates, private keys, and other means of proving one's identity, but, in the United States, they have not been widely deployed. One reason a company might be reluctant to embrace the technology is the trouble and expense of retrofitting the existing corporate infrastructure with smartcard readers. The adoption of smartcards has been anticipated for years, but has been slow in coming, and the trend is likely to continue for corporate PCs.

Wireless phones, on the other hand, and other handheld devices, may soon come equipped with a slot for a smartcard, which will make the adoption of the technology much easier and much more acceptable in the wireless world.

Two new specifications in WAP 1.2 address these limitations.

- WMLScript Crypto library specification
- WAP Identity Module (WIM) specification

The WMLScript Crypto Library provides the means for cryptographic functions to be initiated on the WAP client from the content provider's Internet web site. Mr. Imbert says, "It is an end-to-end security mechanism. Within WAP 1.2, the WMLScript Crypto library provides the digital signature [from the WAP client], and will provide other functions (like encryption/ decryption of small parts of data, or verification of signed contents) in future releases. This first function within WAP 1.2 has a major importance because it solves the non-repudiation issue for the WAP client side . . ."

The WAP Identity Module (WIM) Specification defines the WIM as a tamper-resistant device and as an independent smartcard application. It is clear that implementing the WIM functionality on a smartcard is both appropriate and desirable. The WIM works in conjunction with WTLS, and provides cryptographic operations during the handshake. It is also used for "securing long-living WTLS secure sessions."

A tamper-resistant smartcard is an appropriate place to store and protect "permanent, typically certified, private keys." The WIM uses these keys for such operations as signing and key exchange. The private keys never leave the WIM.

These three specifications, WTLS, WMLScript Crypto Library, and WIM act together to provide the desired foundation for conducting e-commerce transactions across wireless networks: privacy, data integrity, authentication, non-repudiation, and end-to-end security.

Other ways of eliminating the Gap in WAP are also under consideration, including the use of proxy servers.

In the October issue of Information Security Magazine, Edmund X. DeJesus reports,

© SANS Institute 2000 - 2005 Author retains full rights.

"The WAP Forum, a coalition of vendors that support the standard, says that WAP 1.3 will eliminate the WAP gap via a client-side WAP proxy server that communicates authentication and authorization details to the wireless network server. WAP 1.3 is scheduled for public release sometime in 2001."

It is encouraging to see that security has been a major initiative of the WAP Forum right from the beginning. Isn't this what we've wished for after seeing so many security afterthoughts get patched into one network after another? Somebody is finally doing it right, but is it enough?

WAP is not without its critics, and many say that it is only a temporary solution that will fade away in a couple of years.

Nick Jones of the Gartner Group says, "We see WAP as a 'tactical' technology that will be absorbed by 2004 as the poor bandwidth and latency deficiencies of mobile networks are resolved." He added that Java will be one of the technologies that sidelines WAP, because it provides superior usability needed for functions such as maps, device independence and, crucially, better gaming opportunities. He said that as more sophisticated handsets come to market WAP will be seen as "the lowest common denominator" for service delivery.

I-MODE

NTT DoCoMo's I-Mode is widely used in Japan, and is branching out to Europe and the USA. It is also providing serious competition for WAP.

I-Mode is a proprietary service that allows users to connect directly to the Internet using Compact HTML (CHTML). It is a packet-switched service and is "always on." Users are charged only for downloading data. Most other wireless networks are circuit-switched and users are charged for connection time.

Eurotechnology is a management firm in Tokyo that plans, supports, and implements high-tech business projects between Europe-Japan and USA-Japan. The following statistics are taken from their I-Mode FAQ:

> At present (November 2000) the world's wireless internet users are distributed approximately as follows:
>
> - 81% of the world's wireless internet users are in Japan
> - 12.5% of the world's wireless internet users are in Korea
> - 5% of the world's wireless internet users are in Europe
> - 1% of the world's wireless internet users are in the USA
> -
> - Japan: 20 million wireless internet users (imode and WAP)

© SANS Institute 2000 - 2005 Author retains full rights.

- Korea: 2-3 million wireless internet users (WAP)
- Europe: 1-2 million wireless internet users (WAP)
- USA: 0.5 million wireless internet users (WAP and PALM)
- Japan: 4 million WAP users
- Korea: 2-3 million WAP users
- Europe: 1-2 million WAP users
- USA: 0.2 million WAP users

Information about security in I-Mode is very sketchy. The following statements are all that exist in the Eurotechnology FAQ on I-Mode Security. Unfortunately, they don't say anything more than "security is important."

- **Why is security an issue on imode?**
  Mobile commerce (mcommerce) is conducted on imode including mobile banking and security trading, therefore security is a serious issue.

- **Which kind of security issues are there on imode?**
  The security issues on imode are divided into different sectors:
  (1) Security of the radio link between imode handset and the cellular base station (this link uses proprietary protocols and encoding controlled by NTT DoCoMo.
  (2) Security of the transparent public internet connection between imode sites and the handset in the chtml layer.
  (3) Security of private networks on imode.
  (4) Security of private network links between the imode center and special service providers such as banks.
  (5) Password security.
  Each of these different security issues needs to be addressed separately.

One message from a mailing list said that since NTT would not publish any information about I-Mode security, it should not be considered encrypted or secure. Without more details, what choice do we have?

NTT is aggressively pursuing partnerships in Europe and the United States, most recently with AT&T Wireless. There is no guarantee that I-Mode will meet with the same success in Europe and the USA that it enjoys in Japan, but it would be sad to see it become the choice of the people if it does not have adequate security. We will end up patching I-Mode the way we have patched thousands of networks before.

Krithi Aiyappa of ciol.com provides us with a closing comment that looks on the bright side. "Another school of thought is that in future the two could join forces to work out a new standard where they would be compatible. A step in this direction could be the fact

© SANS Institute 2000 - 2005 Author retains full rights.

that NTT DoCoMo has become a very senior WAP forum member. . . [and] the next version of WAP could be a combination of the two. So a new standard might emerge where the two will be compatible and this means good things for technology as well as mobile users."

Bibliography

Aiyappa, Krithi. "WAP Vs I-Mode: The Big Fight." Cyber India Online Limited. September 21, 2000.
URL: http://www.ciol.com/content/search/showarticle.asp?artid=16994 (2 Dec 2000)

DeJesus, Edmund X. "Locking Down the Wavelengths." Information Security Magazine. October 2000. URL: http://www.infosecuritymag.com (2 Dec 2000)

Fasol, Gerhard. "Frequently asked questions about imode."
URL: http://www.eurotechnology.com/imode/ (2 Dec 2000)

Imbert, Patrick. "Smart Cards – Enabling Secure Transactions Over Wireless Internet." The Operator Guide to WAP. URL: http://www.wapcongress.com/directory/pages/smart (2 Dec 2000)

Leyden, John. "Java Will Displace WAP, says Gartner." Gartner Symposium/ITxpo in Florida. October 20, 2000. URL: http://www.vnunet.com/News/1112832 (2 Dec 2000)

Newman, Mark (Editor). "Mobile Giants Battle for Applications Supremacy." The Operator Guide to WAP. URL: http://www.wapcongress.com/directory/pages/smart (2 Dec 2000)

WAP WIM. WAP-198-WIM. Version 18-Feb-2000. Wireless Application Protocol Identity Module Specification. Part: Security.
URL: http://www1.wapforum.org/tech/terms.asp?doc=WAP-198-WIM-20000218-a.pdf (1 Dec 2000)

WAP WTLS. WAP-199-WTLS. Version 18-Feb-2000. Wireless Application Protocol Wireless Transport Layer Security Specification
URL: http://www1.wapforum.org/tech/terms.asp?doc=WAP-199-WTLS-20000218-a.pdf (1 Dec 2000)

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.