WAP, m-commerce and security

Is history repeating itself? Security in m-commerce could be in as much disarray as e-commerce was in its infancy. Mark Osborne's paper discusses some of the dangers and hazards of m-commerce and gives a timely insight into what is necessary in ensuring customer confidence.

Mark Osborne is Director of Security Engineering at KPMG. Mark has substantial technical experience in Internet, e-commerce and m-commerce security, having developed many of the technical security services at KPMG. He has an in-depth knowledge of many commercial firewalls, Intrusion Detection Systems and PKIs. He established KPMG's Security Engineering team six years ago to meet the need for practical best-practice e-commerce security, before the term e-commerce security was popularised. This team has a long track-record of success in delivering implementation and assurance services to most leading UK financial institutions.

Mark Osborne
KPMG

WAP, M-COMMERCE AND SECURITY

Mention e-commerce and everyone always thinks of the Internet, web browsers and Amazon.com. Similarly, if you mentioned Internet security all IT people and many non-IT people would think of firewalls, encryption and computer viruses. The field of Internet security is still an expert field but the ground rules and parameters of the discipline, even though constantly rippling, are well defined and generally understood.

Conversely, m-commerce security and more particularly WAP (Wireless Application Protocol) security appears uncodified and largely unquantified. On attending a workshop or expert master-class, you find your self answering more questions than the master, or alternatively drowning in a mist of WAP specification numbers and what they promise in the future. What is the situation now?

This paper aims to set-out a brief and clear description of the technical risks of WAP security, now, today. It covers device security, WAP server security and different methods of authentication.

DEVICE SECURITY

The phone

Everybody knows and is familiar with mobile phones. Within the design, there are a number of high quality security features. The most important of these are:

- a built-in password mechanism, which will lock after 3 or 5 mis-typed attempts;
- an industry approved, tamper-proof smart-card – the SIM-card.

For those of you who have ever forgotten your password, you will be very aware that these functions work. As a comparison, if you built an Internet bank that required a password and a smart-card to gain access, you could be content in the knowledge that your authentication mechanisms were superior to most offerings.

This flawed analysis is at the heart of the misunderstandings over WAP security:

- The SIM and the phone are (nearly) always stored together and the phone is an every day utility object that is easily lost or stolen.
- Time-outs and key-locks are often not used on phones – this means that as long as the phone remains turned on the strong password system will be bypassed. This was exemplified last year by a warning from the emergency services, which stated that the number of erroneous calls caused by people not using a key-lock on their mobile phone was becoming a major problem.
- The default passwords for mobile phones are often commonly known and never changed by the owner.
- All WAP data (at least in some popular handsets) is stored in the phone's memory, NOT the SIM card; this will include login and password information.

These factors certainly diminish confidence in the phone as a secure device.

It is recommended not to design applications that allow access to high risk applications or networks based on access to a particular phone, certificate-on-a-phone or telephone-number alone. If you do and the device is stolen, the customer will lose more than just their phone – they are losing a device that can access sensitive information.

The phone's software

The main security software component on a WAP phone is the WTLS (Wireless Transport Layer Security) portion of the stack. This protocol is the WAP equivalent of SSL (Secure Socket Layer) and it will provide authentication, encryption and integrity services. WTLS supports some familiar algorithms like Diffe-Hellman, RC5, SHA1, IDEA. It also supports some trusted methods like DES and 3DES but it does not however support Blowfish and PGP.

The protocol which provides for three classes of session can be seen in Table 1.

This is all very secure and appropriate. However, this is the vision, not the reality – all these features will not be fully in-place until WAP1.2 and probably will not be seamless until WAP1.3. What is really available now?

In the UK at the time of writing (summer 2000), there are in the order of ten common WAP-enabled phone models from four or five manufacturers. Some of the most popular phones on the market have no documentation available about their security capability. Additionally, some of the phones available do NOT support WTLS. The lack of documentation on this matter leads to confusion about the security available for WAP.

Commonly, the terminals available on the market exhibit the following properties:

- They do not support full WTLS at all – some only support class 1 type connections – none support class 3.
- If they do support WTLS, it is difficult to tell whether a particular session is using WTLS.
- WTLS on many models is disabled by default.
- If your phone does support a class 2 connection and it is presented with a certificate, the information that you receive about that certificate is insufficient to tell whether it is from a valid source. Therefore, most users will accept it – defeating the point of the whole process.

Table 1.

Class	Title	Description
1	Anonymous server client connection	In this mode, only encryption is provided
2	Authenticated server anonymous client connection	Encryption is provided as above – additionally, a client can check that they haven't connected to a bogus server by checking the credentials against a certificate.
3	Authenticated server client connection	As above, but the server can check your credentials against your client certificate.

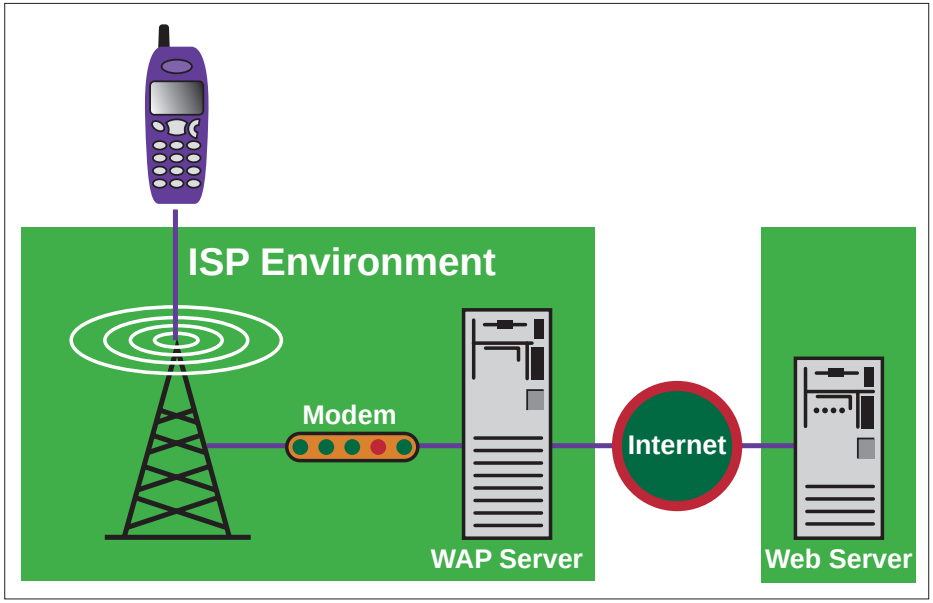

Figure 1. WAP architecture.

Further, WAP supports numerous different encryption and authentication algorithms. It does not define a mandatory cipher suite, therefore there is no guaranteed common set of algorithms between the client and gateway. As a result, there may be interoperability problems between the handset and gateway.

Class 3 relies on the WAP 1.2 specification. This is a finalised specification but it will not be integrated into devices until later in the year or possibly next year.

Not very satisfactory. The bottom-line is that if you are going to do any secure m-commerce trading there must be clear policies and standards so that the customer knows what needs to be done to be secure. You also need to reinforce these with strong legal terms and conditions to protect yourself if your customers choose to behave recklessly.

Viruses – are your WAP devices susceptible?

The current generations of mobile phones are not extensively programmable. So from that perspective they should be quite resistant to a traditional virus – the next generation of mobile-enabled PDAs, which are extensively programmable, will almost certainly be exposed to virus and malicious activity. The Java-enabled phone may also be susceptible to such attacks, as seen in regular web browsers. Java, however, segregates itself from the operating system by means of a "sandbox" and has traditionally been thought of as more resistant than other implementations of active code.

However, if we expand the term virus to include the reception of a script or a message that changes the content of your phone, the risk increases. There are two mechanisms that could cause this:

- SMS provisioning – it is possible to send an SMS message that could reconfigure your phone. This could be used to change your WAP gateway definitions to point you to a malicious gateway that could capture private information.
- WTA – the Wireless Telephone Application interface that is available in a WAP phone. This has the capability of deleting, changing or adding entries to your phonebook, or more.

Some European WAP application providers make it clear that they do not use unsolicited SMS and WTA functions to alter phone settings and recommend that:

- the user contact the network operator if they receive one;
- the user reply "no" to the action messages dialogue.

From an organisation's point of view there is a risk that a WAP system could pass on a virus. There are general products and specific WAP products designed to deal with viruses that should be installed on vulnerable servers and systems.

THE SERVER ENVIRONMENT

The background

Connecting to the Internet on a mobile phone follows these basic steps:

1 User accesses his WAP browser and opens a specific URL
2 The user initiates a connection & transmission from phone via GSM like any other mobile phone. The transmission leaves the wireless network and travels along a PSTN (land-line) network.
3 The modem answers the call and establishes connectivity with PPP just like connecting from your home PC to your Internet service provider
4 The phone is assigned an IP address and contacts the WAP server or gateway
5 The WAP server finds the relevant web server and obtains the data
6 The connection between website is standard HTTP
7 The WAP server returns the data to the phone in WAP format

When a secure session is initiated, the connection between the WAP server and the WAP browser is protected by the WTLS. The connection between the WAP server and the Web server is encrypted using the facilities of SSL, as in a regular secure website. However, there is no end-to-end encryption and whilst on the server the transmission will spend some time in clear text. This is known as the WAP GAP and it is shown in Figure 2.

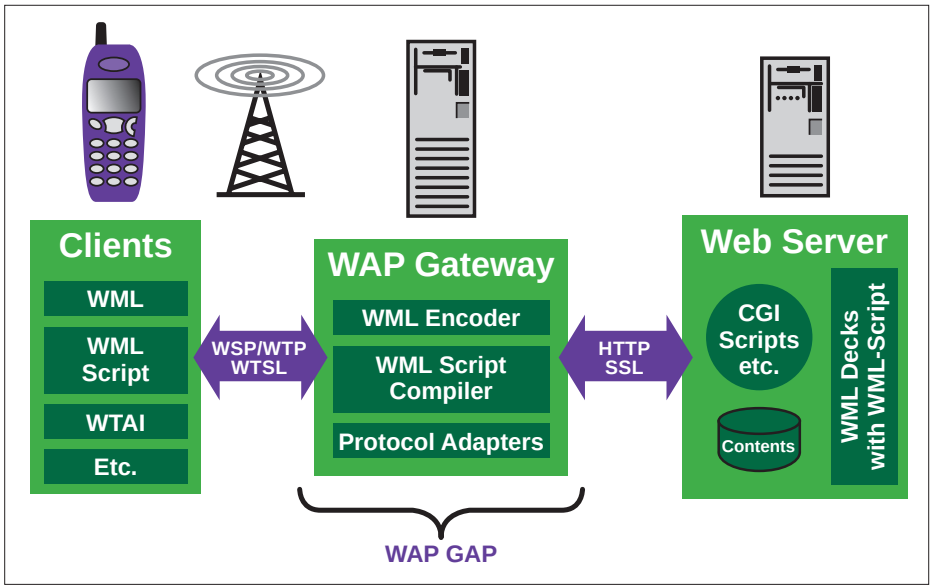

Figure 2. WAP GAP model.

Network operator-managed WAP servers

In the network operator-managed model (Figure 1), the WAP server is managed, owned and run by the network operator. This simplifies configuration of handsets and operation but it does expose the user to the risks shown in Table 2.

Owner-managed WAP servers

The second generic model is the owner-managed WAP server (Figure 3). Here all the components are

Table 2.

Description	Likelihood
A WAP operator (or a malevolent intruder) views confidential information in the memory of a WAP server while it is being converted from SSL to WTLS	Possible – but quite difficult
A WAP operator (or a malevolent intruder) could turn off WTLS and view private authorisation details with a packet sniffer	Easy – additionally, poor handset design would make it difficult to detect
A WAP operator (or a malevolent intruder) could turn off SSL and view private authorisation details with a packet sniffer	Easy – but may require a little planning so unlikely to be a hacker
A WAP operator (or a malevolent intruder) could redirect requests intended for your website to a dummy application, inserting advertising or capturing client authorisation details	Possible on most WAP servers – very simple on some
A WAP operator (or a malevolent intruder) could view confidential information using audit logs	Possible
A WAP operator could gain "profile" information like transaction times, volumes and location for commercial advantage	Possible

It should be noted that we have exploited all these exposures in lab conditions.

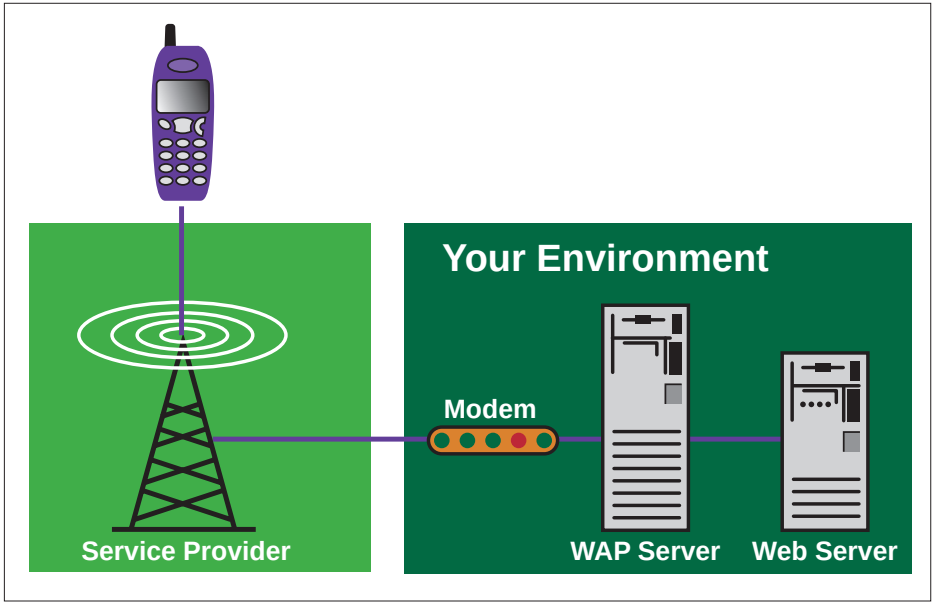

Figure 3. Owner-operated WAP gateway.

located on the application provider's site. This has been more popular with organisations that already have an investment in a large modem pool, like those with a sizable legacy no-internet PC banking application. Obviously, the WAP server is still vulnerable to all the above risks but in this case the application provider can impose its own security regime to counter the threat. This may include access control, audit software and intrusion detection.

The risks in this environment include those shown in Table 3.

A slight variant on the completely owner-managed WAP configuration is shown in Figure 4. Here the WAP server is located on the provider's site but the modem pools are located on a telecom provider's site. The risks here are the same as any other Internet application and therefore can be countered by prudent use of firewalls and routers.

Table 3.

Description	Likelihood
A malevolent intruder will penetrate your network through the modem pool designed for WAP access	Very possible – the WAP modem is an ordinary modem. Without proper firewalls there is a real risk.
Virus	Easy – just send a copy of "I love you"

Authentication methods

This is likely to be greatest area of change in m-commerce WAP and m-commerce arena. PKI, which is rapidly becoming a common technology, will be important in the WAP authentication. This will bring with it yet another acronym, M-PKI. This will coincide with the emergence of WIM, Wireless Identification Module, and the wide-spread client-side Public key certificates. This will be with us in the UK soon, with some deployments during 2001. How rapidly it is used will depend on the take-up of WAP1.2 phones.

With the current technology, there are also security risks associated with the type of authentication you use.

- Most WAP browsers have an "ease of use facility" which will request that a user ID and password are stored and automatically used when prompted for a password.
- This prompting is very persistent and will ask continually – so it will take a strong-willed user to resist.
- Given the size and ease of loss of most mobiles, this facility will make the user ID and password method of authorisation almost pointless.

We have spoken to some technicians who have noticed a potentially worrying phenomenon. Apparently, on certain occasions when a user authenticates to a certain site (SITE A) with authentication credentials (user ID and password), then immediately switches to another site (SITE B) which also requires authentication, the WAP server can present the user ID and password from site A to site B. We have not replicated this problem but potentially it could be serious as it could allow for user ID and password stealing. Some years back many Internet proxy servers suffered from a similar problem, so the symptoms appear entirely credible. However, it could be a manifestation of the browser problem described above.

Some WAP gateways have facilities that can allow access by identifying a specific device number (telephone number) or IP address.

Often these can be unavailable or meaningless, leading to some pointless or insecure definitions.

CONCLUSION

We hope this is a clear concise discussion of the security risks of the WAP environments of today – not tomorrow or at some undefined point in the future. Those that are sensibly investing in WAP services may have found this information difficult to find. Listen to conversations on the subject after reading this and other material; you will surely find many of those speaking or writing on the subject confused or inaccurate. Similarly, the discussions of future developments seems surrounded by a mist of confusion.

Some believe WAP is an interim technology, and are reluctant to dip their toes in the vast ocean of m-opportunity. This is based on a lack of understanding – these organisations are heaping all manner of blame on the poor infant WAP, making it guilty of poor phone design, poor market positioning by the telecoms companies, and a

business which is being swamped by "too much quality, not enough depth". This paper is intended to be the first of many actions on our part to redress this balance. We think that WAP is an emerging technology, like the 486 PC and Windows was all those years ago. And we believe that those who invest in WAP early, like those who learnt to manage the Internet in the early 1990s, will become the masters of more complex 3G technology.

GLOSSARY

Bearer

A telecom service that is used to carry data from WAP-enabled terminals to the WAP server through the wireless network.

HTML (HyperText Markup Language)

A subset of Standard Generalised Markup Language (SGML) used on the World Wide Web. HTML defines the page layout of a WWW-page, ie fonts, graphic elements and hypertext links.

HTTP (HyperText Transfer Protocol)

A protocol utilising TCP/IP that enables the transfer of HTML files. HTTP is used in WWW services.

HTTP proxy authentication

Some servers require the user to authenticate himself/herself in order to receive content. Usually a username/password combination is required.

IP number/address

A numerical identification number individualizing a data processor or a data transferring device connected to the Internet or a network connection.

ISP

Internet Service Provider. Companies that provide connectivity to the Internet for businesses and domestic users.

Java Script

A de facto standard language that can be used to add dynamic behavior to HTML documents.

MSISDN (Mobile Station International Subscriber Device Number)

An ISDN number which uniquely defines the mobile subscriber on an international level. An MSISDN consists of three parts: the country code, the national destination code and the subscriber number.

PPP

Point to Point Protocol. A wide area networking protocol often used by modems when connecting to LANs.

Proxy server

A server that records frequently-used files so that it is not necessary to retrieve them from their original location every time a workstation sends a request. For example, when using the Web, the proxy speeds up the downloading of web pages located behind slow or congested network connections.

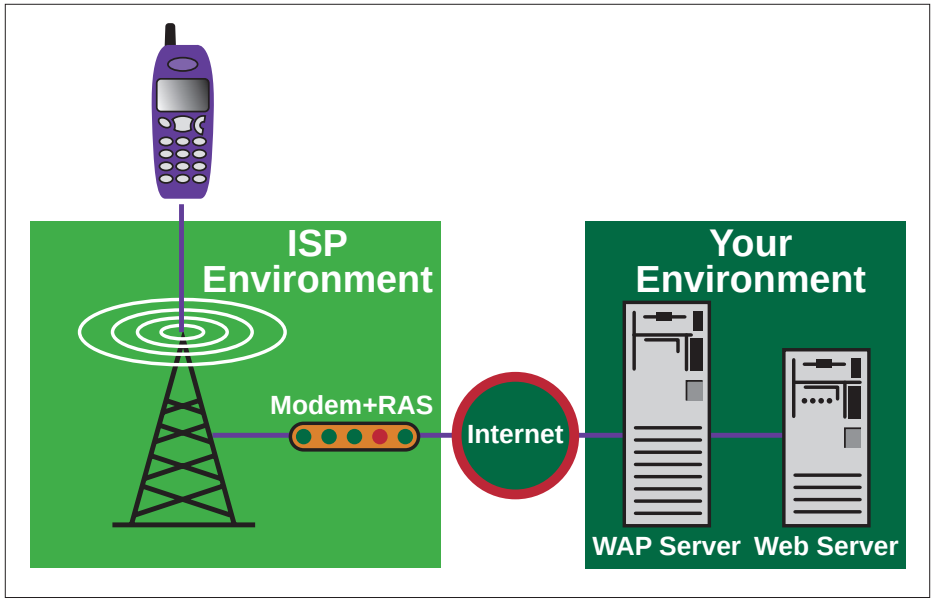

Figure 4. Hybrid owner-managed configuration.

Ras/Dial-up server

A device that allows remote users to connect to the local area network or to the Internet.

SMS

Short Message Service. System used to send short text messages from one mobile phone to another.

SSL

Secure Sockets Layer. Protocol for encrypting data sent across the Internet and for authenticating Web servers. Often used in WWW to secure credit card transactions.

TCP/IP

Transport Control Protocol / Internet Protocol. The communications protocol used on the Internet.

WAP

Wireless Application Protocol
Protocol optimised to deliver Internet services to mobile devices over low bandwidth networks.

WAP Browser or Micro Browser
Software loaded onto client mobile device that displays pages. Similar in function to IE or Navigator.

WAP Gateway or WAP Server
Software that translates WAP into Internet protocols and acts as a proxy for WAP devices.

WML

Wireless Markup Language. XML based mark-up language designed to be read by WAP browsers.

FURTHER INFORMATION

CONTACT:	*Mark Osborne*
COMPANY:	*KPMG*
ADDRESS:	*One Canada Square* *Canary Wharf* *London* *E14 5AG* *UK*
E-MAIL:	*mark.osborne@kpmg.co.uk*
TEL:	*+44 (0)20 7311 5468*
Mob:	+44 (0) 7802 445507