

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

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.

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 uncoded 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.

