IBM Global Services
July 2001

A security strategy for mobile e-business

Managing risk, protecting privacy and securing trust in the wireless revolution

Daniel Keely
EMEA Wireless Security Competency Leader within the IBM Security and Privacy Services organisation

Key Topics

- ***Assesses the significance of security and privacy in relation to the latest developments in mobile e-business***
- ***Outlines the key challenges in developing secure wireless services and highlights the new risks and threats that mobile e-business creates***
- ***Details the pros and cons of a range of existing and forthcoming security standards and solutions***
- ***Explores strategies and key steps for building the solutions, processes and security organisation to meet the challenges created by wireless applications***
- ***Provides a road map towards planning and developing security measures to safeguard the success of your mobile e-business.***

Executive summary

Mobile e-business presents companies with both an exciting business opportunity and a massive challenge. From offering consumers the convenience and flexibility of mobile services anytime and any place, to extending your enterprise applications and data to today's roaming workforce, mobile e-business offers new ways to generate revenue, streamline core processes and reduce costs. At the same time, mobile e-business also brings all the complexities and risks associated with developing new business models within 'uncharted waters'.

Security is arguably the greatest challenge companies face in realising these opportunities. Mobile e-business exposes companies to a massive range of new threats and vulnerabilities. Their ability to address these risks will be crucial to brand image, customer confidence, market penetration and the long-term success of their mobile e-business strategy.

In addressing these challenges, companies need to understand how wireless e-business differs from the normal enterprise environment. For one, mobile e-business brings increased complexity. In the new wireless environment, security will encompass issues as diverse as privacy, data integrity, ease-of-use and application availability. On another level, security also needs to address multiple devices, multiple operating systems, the complexity of the path for transactions and the sheer number of parties involved. The only way to succeed in mobile e-business is to develop an effective end-to-end strategy for assessing and managing each of these complex risks.

This paper outlines the key challenges in developing secure wireless services that address the new risks associated with mobile e-business. It assesses the threats that arise with wireless transactions and highlights the most important technologies and trends in the evolving field of wireless security. There is also a discussion of some of the most appropriate security controls, as well as initial guidance on how to apply these as part of a long-term security strategy.

It is difficult to overestimate the importance of an effective security strategy to the long-term viability of any mobile e-business initiative. Companies need to start addressing these challenges now to ensure security becomes an enabler rather than obstacle to success.

Opportunities and risks in the world of mobile e-business

Mobile e-business is about to become commercial reality. Mobile phones and increasingly other wireless devices – Personal Digital Asistants (PDAs), Webpads, Pocket PCs, embedded devices – are becoming ubiquitous, reflecting an increasingly mobile lifestyle. Today everyone takes the ability to 'stay in touch' on the move for granted. Now many people want to go a step further – to be able to make purchases, access services and transact business from anywhere and at anytime, using a range of mobile devices.

A large number of these services are being piloted today and the move to 2.5G and 3G will open up a huge range of possibilities. For example, the airlines are trialing a service which lets you check-in for flights using your phone; retailers are piloting location based services that allow them to target consumers phones with personalised promotions when they are in the vicinity of a store. Other initiatives will allow people to pay for products using their mobile devices. In addition to these business to consumer (B2C) opportunities, many businesses see the next generation of mobile services as a way to improve collaboration and efficiencies across the virtual organisation.

There are many other mobile e-business applications in the pipeline. However, virtually all these models presuppose a high level of security to be successful. It is well recognised that one of the biggest obstacles to mobile e-business is winning the trust of the customer and a single security breach is a very high profile way of undermining everything the company has been working for. Success therefore depends on developing a security strategy that addresses the new and complex challenges of mobile e-business.

A gap in the defences

Security is becoming a major business issue. The recent spate of 'Denial of Service' attacks, in which hackers deliberately overload a company's Web servers, is just one example of how serious and damaging the threat can be. However, in mobile e-business, these threats are likely to become more prevalent and many times more complex.

The trouble is that existing security controls (such as those embedded within wireless networks) are not adequate to deliver the levels of security that the next wave of mobile e-business will demand. Moreover, companies will not be able to rely on third parties to provide security, for instance, connectivity suppliers cannot and will not guarantee end-to-end security for your mobile transactions.

The security issue also has many dimensions in mobile e-business that adds to this complexity. Any security strategy will need to encompass issues such as privacy, data integrity, the balance between adequate security procedures and ease-of-use and the availability of mission-critical services and applications. On another level, security needs to address multiple devices, multiple operating systems, the complexity of the path for transactions and the sheer number of parties involved.

Managing these risks and challenges – it will be your responsibility to do so – is a massive challenge. All of these factors, many of which are unique to mobile e-business, must be adequately considered and addressed before rolling a mobile e-business service out to the customer.

Trends and developments in mobile e-business

Before embarking on a more detailed discussion of these challenges, it is worth highlighting some of the key developments in mobile computing.

WAP and GSM technology: WAP provided the first opportunity to develop simple mobile e-business services. However, while WAP has allowed users to browse information using mobile devices, bandwidth and device limitations make WAP less suitable for supporting business transactions and take-up by users has been relatively slow. As WAP is not generally used for wireless payments or critical business transactions, there has been little need for (and not much attention given) to the issue of security.

2.5G and GPRS: Wireless networks are evolving from voice only networks into general purpose data networks. This is being accomplished technically by migrating from circuit switched technology to packet switched technology, and as a first step the GSM network is being enhanced with packet switched GPRS technology. 2.5G, an interim step before 3G (third generation network), will also offer 'always on' connectivity and will have the bandwidth capacity to support, for the first time, practical mobile e-business transactions. As such, the issue of security will become crucial.

3G and UMTS: Universal Mobile Telephone System will be a packet switched only network which offers the prospect of a global wireless standard for mobile e-business. 3G should also offer sufficient bandwidth and performance to support highly sophisticated, data-intensive mobile e-business applications. For both 2.5 and 3G, the volumes and sensitivity of data exchanged in mobile e-business will increase massively, creating the need for much higher levels of security.

Wireless LAN: Wireless Local Area Networks represent another important (but often overlooked) element in the wireless environment. Wireless LAN is already widely deployed by companies, who find it a more cost effective and flexible way of supporting trends like 'hot desking' and the flexible provisioning of mobile services. However, wireless LAN deployments often feature very little security control and potentially present a 'backdoor' gateway to gain unauthorised access between mobile device and corporate data, systems and networks.

Bluetooth and PAN: Bluetooth and Personal Area Networks (PANs) will provide a cost-efficient and simple way of connecting a wide range of mobile devices and intelligent appliances within the range of approximately ten metres. It is likely that Bluetooth will be widely deployed and again without adequate security measures could provide a backdoor route for unauthorised access to your corporate data and systems.

Mobile devices: Current mobile devices, such as PDAs and cellular phones usually offer very little native security and are severely constrained in terms of memory, processor speed and storage capacity. As a result, it is a challenge to implement today's resource intensive security measures on these devices. However, technology developments will start to offer improved security controls within the constraints of the mobile device environment in the near future.

Key security issues in mobile e-business

Security can be broken down into a number of key issues, as follows:

Confidentiality: The confidentiality of sensitive information such as credit card details needs to be protected. Unauthorised people should not be able to gain access to confidential material – yet there have been a number of high profile e-banking cases where this has happened with serious consequences for brand image.

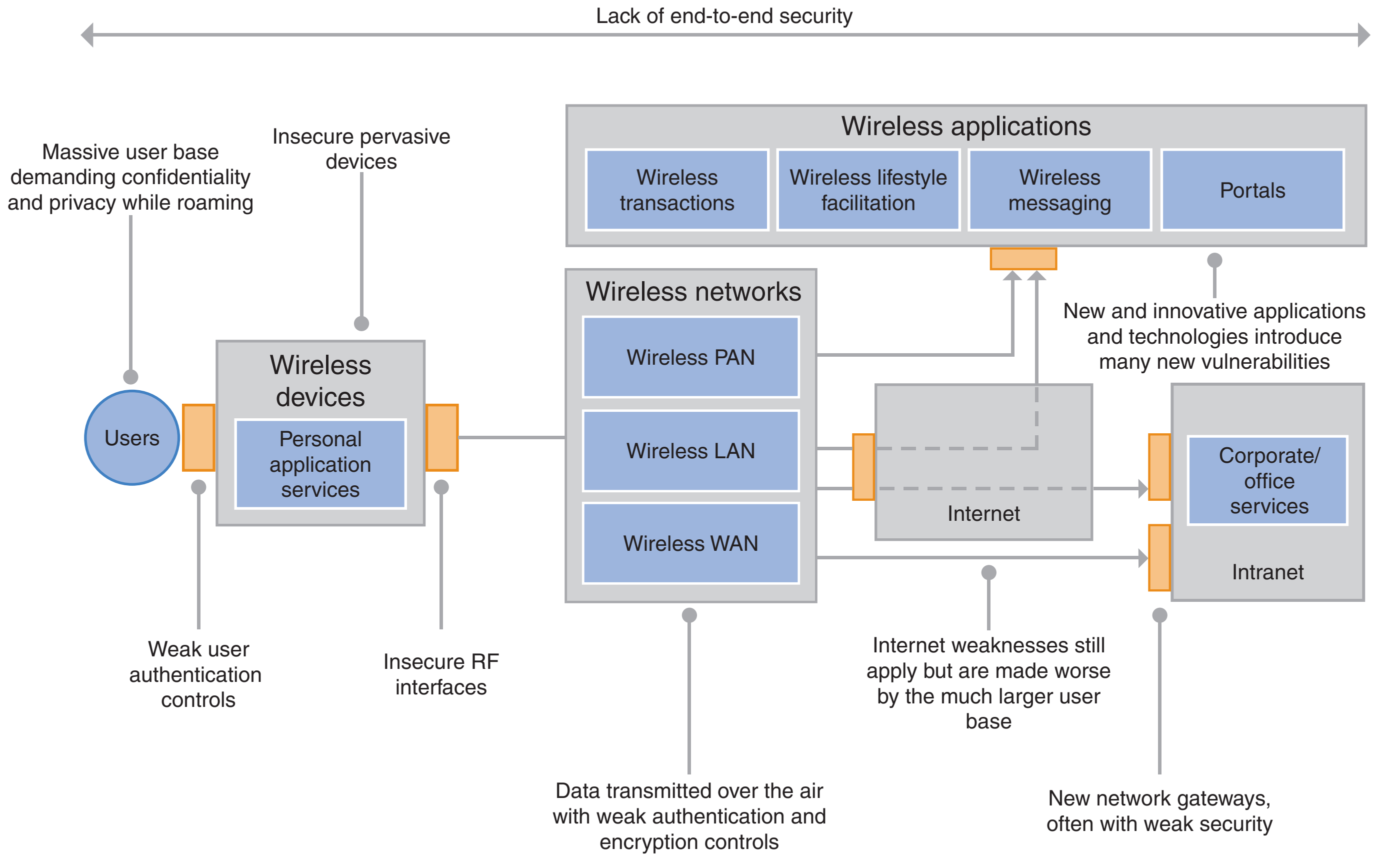
Integrity: Companies need to protect the integrity of data transmitted over wireless networks from the point of transmission to the point of delivery. This is particularly essential for financial transactions – so, for example, if a user enters a payment for $10, this amount must not acquire an extra zero in transit. To address this risk, it must be possible to check that the data is the same at the points of origin and destination.

Availability: This is about ensuring that mission critical data and services are available on demand, which today often means 24 hours a day, seven days a week. This is closely interlinked with security because a security breach can lead to downtime, as in the case of Denial of Service and virus attacks. If your systems are not secure against unauthorised interventions (whether malicious or not), there is a risk that your service will be unreliable and that either employee productivity or customer satisfaction will suffer as a result.

Privacy: In addition to these well-established security issues, privacy will become a prominent issue in mobile e-business, particularly with the development of location based services (see below). Companies will also need to meet the legal requirements of Directive 95/46/EC of the European Parliament concerning the processing of personal data and the free movement of such data.

New threats, new challenges

The wireless e-business environment is very different to the wired environment. In mobile e-business, your security measures will come under more stress and be vulnerable to an unprecedented range of abuses. It is crucial to understand what these threats are and to plan a strategy to manage them. This section will go on to consider some of these new threats in more detail.


Lack of end-to-end security
Massive user base demanding confidentiality and privacy while roaming
Insecure pervasive devices
Wireless applications
Wireless transactions
Wireless lifestyle facilitation
Wireless messaging
Portals
Wireless networks
Wireless PAN
Wireless LAN
Wireless WAN
New and innovative applications and technologies introduce many new vulnerabilities
Users
Wireless devices
Personal application services
Internet
Corporate/ office services
Intranet
Weak user authentication controls
Insecure RF interfaces
Internet weaknesses still apply but are made worse by the much larger user base
Data transmitted over the air with weak authentication and encryption controls
New network gateways, often with weak security

As this diagram shows, there are numerous new points of vulnerability within the wireless e-business environment.

The range and nature of the threats will vary hugely depending on each application and the environment in which it operates. However, the following points illustrate some of the typical threats and challenges that mobile e-business presents:

- ***Increased complexity.*** *It is difficult to assure the confidentiality and integrity of a company's data as it is exchanged over wireless data networks involving many different third parties. Mobile devices are the new interfaces to e-business applications, yet their security capabilities are severely restricted.*
- ***New virus risks.*** *The variety and immaturity of wireless devices, operating systems, applications and network technologies as well as the size of the user base increases the threat of virus and malicious code attacks.*
- ***Password vulnerability.*** *The initial access code or password on wireless devices can often be deactivated by the user and allow unauthorised access to applications and data.*
- ***Unauthorised reconfiguration of device.*** *Wireless devices may have Over The Air (OTA) remote configuration facilities, undocumented APIs or software bugs that could be exploited and abused.*
- ***Denial of Service Attacks.*** *By continuously transmitting large amounts of data to the wireless device, network bandwidth may be saturated and the battery on the device drained leading to performance degradation or non-availability.*
- ***A weakness in WAP.*** *WAP does not provide end-to-end encryption. The data is available without protection at the WAP gateway. This may result in unauthorised information disclosure or non-compliance with industry regulations (e.g. banking).*
- ***Unwanted data.*** *With GPRS 'always on' connectivity, most billing models offered by wireless operators charge for packets of data both transmitted and received. This means that a device being bombarded with unwanted traffic would result in the owner of the device receiving a large bill.*
- ***Loss of data.*** *Storage capabilities of mobile devices are increasing. If a device malfunctions, is lost, or if its data is accidentally deleted and there is no recent data backup combined with restore capability, the data will be lost forever.*

- ***Bluetooth as a hidden gateway.*** *If a device is equipped with Bluetooth connectivity as well as a GSM/GPRS interface it may be possible for an unauthorised user to access the device in proximity and 'gateway' through to an existing connection to a private network/intranet.*
- ***Signal jamming.*** *Radio frequency signal jamming in the proximity of the device or a base station can lead to disruption and non-availability of wireless devices and networks.*
- ***Duplicate SIM cards.*** *Specialist equipment is available for cloning SIM cards. The use of duplicate SIM cards can lead to call fraud. If application security is based on user authentication to the device (from the SIM) then it will also be possible to masquerade as a genuine user.*
- ***RF Scanners.*** *The combination of data being transmitted over public radio frequencies and the weaknesses in the cryptographic algorithms gives rise to digital RF scanning equipment capturing and decrypting data, leading to loss of confidentiality and information disclosure.*
- ***Loss or theft of device.*** *Mobile devices are carried outside the office, and their size means they are easy to misplace. Since mobile devices generally have very limited security features built in, losing them also means that sensitive corporate or personal data may be disclosed.*
- ***Location-based services.*** *Mobile e-business delivers location based services, which will enable users to be tracked. This introduces new privacy and confidentiality concerns for consumers.*
- ***The window of opportunity.*** *'Always on' connectivity increases the window of opportunity for unauthorised access to your systems, and because mobile devices can be accessed even when they are not actively in use, users are less likely to know if they have been a victim of an attack.*
- ***Non-repudiation.*** *For financial transactions, companies will need to be able to assure 'non-repudiation' – in other words, to prove that a mobile transaction actually took place.*
- ***Immature security controls.*** *The rapid development of new mobile technology means that it is not always mature or suitably verified for security. There are also a lack of standards for user and device authentication, executable content security and stored data security.*

These risks could lead to data and applications being accessed, destroyed, manipulated or copied by an unauthorised person. Confidential and personalised data may be disclosed and modified and there is also the risk that customers privacy rights could be abused and the business could be a target for fraudulent activities. Some of the risks also lead to disruption or non-availability of the wireless devices and networks, with potentially serious consequences to mission critical operations.

Privacy and the impact of location based services

In addition to the threats outlined above, the development of location based services will have far-reaching implications regarding individuals' privacy rights.

In mobile e-business, new information concerning individuals (namely location information) will be processed by service providers which potentially are not communication carriers. Moreover, this information will be combined with customer intelligence, leading to concerns that individuals may be losing control over their personal, sensitive information.

At the simplest level, location based advertising consists of sending an advertising message to every user who enters a certain perimeter. Of course, this service will not be appreciated by everyone and so the ability to opt out will be essential.

In a more sophisticated scheme, location based advertising would be carried out only if the contents of the advertising message meets the users interests. A similar service would consist of letting a user know when they are in the vicinity of another user who shares common interests. In both these cases, somebody (or some system) has to have access to both location information and information specifying the user's interests. The question is, who should have access to this information, and on what terms?

To take this a step further, over a period of time a mobile device could be used to track an individual's location and to develop a profile of their movements (and by association, habits). Furthermore, with the introduction of UMTS, location information will become more precise, while 'always on' connectivity potentially enables round-the-clock traceability.

This kind of information is very valuable, but if abused can be very damaging to customer relationships. Given the sensitivity of this kind of information, people will want to know that their information is in safe hands before they will consider adopting location based services. It is therefore essential that organisations develop transparent rules and policies about who has the right to process what information, and for what purposes.

Managing risk

In this chapter, we have only outlined a few of the new threats introduced by mobile e-business. Leave any gap and you risk a breach that could cost your business dear.

Of course, it is never possible to completely pre-empt and eradicate all threats. However, success in mobile e-business will depend on having an end-to-end strategy that minimises risks to a level which is acceptable to your company and its customers. Moreover, since mobile e-business is in its infancy, it will be important to develop strategies and solutions capable of evolving to meet rapidly changing requirements and new challenges.

Chapter 2:
Securing a future for your mobile e-business

Given the security issues and threats outlined above, companies need to start planning and implementing strategies to mitigate these risks and develop end-to-end solutions for mobile e-business. Such a strategy will need to be designed around the requirements of each company, its customers and the specific mobile applications. However, all companies will benefit from applying a structured approach to reducing security risks in the mobile e-business.

To a large extent, a company's success in mobile e-business will depend on its ability to manage the risks and challenges outlined in the first chapter. Consumer confidence, brand equity, return on investment and market share and valuation are all linked to one issue: can you guarantee your security strategy is adequate to the challenge of mobile e-business?

The key to meeting this challenge is to have an end-to-end approach to mobile e-business. However, what does end-to-end mean in the case of mobile e-business?

- ***Safeguard every gap.*** *Assure complete data security from point of transmission to final destination(s), covering every stage in between. Don't just look at over the air transmission. Identify every vulnerability and introduce the security and privacy measures needed to assure security at each step in the chain. (Remember, any gap is an invitation to abuse).*
- ***Protect every channel.*** *Up to now, security has mainly been about protecting data transmitted to PCs. Mobile e-business introduces a plethora of devices with different operating systems and standards – security has therefore become a much more complex issue. Companies need practical security solutions that can be quickly and easily modified for a whole range of devices.*
- ***Consider the bigger picture.*** *The security strategy will have an impact on a range of business issues. So it's not enough to look at security in isolation – the mobile devices still need to perform and offer ease-of-use. It's no good implementing a 128 character authentication code if the procedure is so long-winded it discourages users from taking up your mobile services. Equally, issues such as performance, personalisation, scalability, availability and systems management are all-important considerations with an impact on the security strategy.*

To address security and privacy issues across each of these dimensions, organisations need an approach that encompasses security management process, security policy, security technology and the security organisation.

Security solutions

A wide range of security solutions – in the form of processes, technologies and organisation models – exist to address the risks and vulnerabilities of mobile e-business.

To begin with, wireless e-business solutions still require the same security controls that are used to protect the corporate network perimeter and Web applications used in the wired e-business environment. These controls will include technologies such as:

- *Firewalls*
- *Content/e-mail filtering*
- *Anti-virus*
- *User identification and authentication*
- *Authorisation*
- *Policy management*
- *Intrusion detection*
- *Hardened platforms*
- *Secure device management.*

It should also be noted that the wireless environment may push these controls to their limits. This is due to potentially much larger groups of users, with different device types, connecting from different locations.

In addition to these controls, additional technologies will be required to provide security across wireless e-business channels. Many of these technologies for mobile e-business security are in a state of development or evolution. However, there are some key trends and options that companies can consider. These include:

Cryptographic technology

Additional cryptographic solutions are available to reduce the risk of data being intercepted while in transmission over wireless networks. This is necessary because of the known weaknesses in the cryptographic technologies built into GSM and GPRS networks. These solutions operate on top of the existing systems offered by the wireless network operators, but can be controlled by the organisation and use proven and standardised protocols. Options available include IPSEC, WTLS and TPKDP.

IPSEC is mainly targeted at laptop PC clients, although at least one IPSEC VPN client is now available for the Palm. It will become a really viable solution when the mobile devices support IP6 (which includes IPSEC as standard). It uses a standard TCP/IP stack and Web browser (not WAP), although there are some cross-vendor interoperability issues to be aware of.

WTLS is part of the WAP standard and uses RC5 and SHA-1 encryption. It is targeted mainly at PDA and mobile phone devices and provides encryption between the mobile device and WAP gateway. In WAP v1.2 there is support for server side authentication using WTLS certificates.

In addition to WTLS and IPSEC support, IBM Websphere* Everyplace Suite (WES) is able to provide encryption as part of its two party key distribution protocol (TPKDP) using DES encryption. This enables both the device and the server to be authenticated. It also supports both laptop and PDA clients.

Personal Firewalls

Devices attached to 'always on' networks need additional security to prevent unauthorised access. A personal firewall can be installed on a laptop that is always connected to the Internet through a GPRS connection. This can protect corporate and personal data stored locally on the laptop. This technology is not yet available for low-powered devices such as telephones or PDAs.

In addition to controlling suspicious connections, additional protection is needed from inappropriate content. Wireless devices are known to contain many 'secret' instructions that are meant to be used for maintenance purposes by qualified engineers, but are easily exploited by viruses or other forms of inappropriate content. Specially formulated Short Messaging Service messages are known to update SIMs and are able to access functions in GSM mobile phones like the address books. Antivirus and other content filtering software for mobile devices is just starting to appear on the market to combat these issues.

Strong user authentication

For some purposes, particularly financial transactions, strong authentication will be required. To ensure security in the mobile environment there is a strong case for applying 'two factor' authentication (based on something you have and something you know). Conventional two-factor techniques, such as TAN (Transaction Number) codes, can also be used in a wireless environment. Alternative solutions involve handheld one-time password generators (time based) or smartcards (challenge/response). In the case of a smartcard, it can be combined with digital certificates and form part of a Public Key Infrastructure (PKI) (see below).

To replace PIN codes with a stronger form of authentication, biometric user authentication could be considered. This includes finger print, face or retina scans.

Single sign-on

Authentication support should enable single-sign on functionality, so that all of the services and applications of the environment are available to the user without further user-visible authentication. This will require the secure transfer of user credentials from a portal to other systems used to provide content services and applications; this includes third parties.

Wireless PKI technology

Wireless Public Key Infrastructure (wPKI) technology can be deployed to achieve true end-to-end security of the data transmission path, secure user authentication and trusted transactions. wPKI uses public key cryptography and open standards technology to build a trusted security framework that facilitates the authentication of transactions and secure communications over public wireless networks.

Trusted Third Parties (TTPs) utilise PKI technology to issue digital certificates that are used to identify a user. As well as securely authenticating the user and protecting the confidentiality and integrity of data transmission, the trust associated with PKI is also needed if businesses are required to implement non-repudiation so a party cannot falsely claim that they did not participate in a transaction. To make sure this proof is admissible in court, digital signatures are required that are legally binding. Such signatures can be implemented using digital certificates that are issued by a TTP.

Authorisation

Authorisation solutions are responsible for managing and integrating user access control and authorisation information, as well as restricting user access if necessary. Authorisation can be modelled in two ways, either capability based (defined per user according to the resources that can be accessed using subscription profiles), or ACL (Access Control Lists) based (defined per resource which users can access). Simple authorisation checks can be done by various places in the wireless environment (e.g. authentication server, proxy, Web server, and application server). More sophisticated authorisation checks are typically implemented in a separate, dedicated component.

Although the access control in the wireless environment can be implemented using HTTP proxy technology, in general a finer level of access control should be provided. This has to be done at the level of individual components and application servers. Typically, dedicated products have to be integrated with the services of the wireless environment.

Security processes

It should be clear that understanding the risks, building the correct architecture and deploying the appropriate security controls is not trivial and must be managed through a structured process. It should also be clear that security is not just about technology. Sound end-to-end security also requires the appropriate policies, processes and organisation. Such processes would typically include the following:

- *Risk management process*
- *Incident management process*
- *Security validation/assurance process*
- *Security monitoring process*
- *Change management process*
- *Corporate security policy*
- *Security architecture*
- *Technical standards and policies*
- *Privacy policy*
- *User rules*
- *Corporate security organisation*
- *Incident response team.*

A security road-map for mobile e-business

It should be clear by now that security for mobile e-business is not simply a matter of implementing new security controls in isolation. The following steps outline some of the key steps and success factors that are essential to planning and implementing an effective security solution for mobile e-business.

Define clear objectives. Understand the business goals, objectives and critical success factors when planning the security strategy, as well as the impact on the business if they are not achieved.

Identify the points of vulnerability. What are the new threats and risks arising from your specific mobile e-business model? Identify the vulnerabilities in your company's processes, organisation and technologies and anticipate how they could be exploited.

- ***Manage the risks.*** *Determine and measure the risks to the business, then identify security requirements and measures for reducing those risks to an acceptable level.*
- ***Gain executive buy-in.*** *Gain management's commitment to the security strategy. Ensure their approval of what constitutes an acceptable level of risk and their support for the services required to ensure risks do not exceed these levels.*
- ***Formalise the plan.*** *The security strategy needs to be clearly defined, structured and communicated. Formalise the security requirements, policies and processes to avoid the risk of uncertainty or misinterpretation.*
- ***Develop an end-to-end security architecture.*** *Either build a new security architecture, or integrate new mobile e-business controls into the existing Information Technology (IT) architecture. Ensure all threats and vulnerabilities are adequately addressed.*
- ***Implement a business-oriented security solution.*** *Security technologies need to be selected, implemented and configured to match the requirements of your security policies and the broader mobile e-business strategy.*

- ***Test and validate the solution.*** *Evaluate end-to-end security solutions against a variety of threats and scenarios and refine solution accordingly. New threats will emerge, so this should be an ongoing process.*
- ***Establish a review cycle.*** *Operate, manage and audit the solution within a continuous security and risk management process to ensure the 'level of protection' is maintained.*

Delivery – filling the skills gap

One of the greatest challenges companies will face in this area is finding the skills and resources to implement, manage and evolve their security strategy for mobile e-business. There is already a skills crisis in the more established fields of e-business. Finding experience and expertise to address the emerging challenges of mobile e-business will be even harder.

Many companies will need the support of a specialist in this field. But it is crucial that you select the right partner to underpin such a vital area of your business strategy. Given the scope and complexity of this issue, the partner should at least meet the following selection criteria:

- ***Opt for experience.*** *The wireless environment presents a range of unique challenges. Choose a partner with a proven understanding of the issues, and with experience of delivering solutions in the field of security and wireless e-business.*
- ***Tap into breadth of expertise.*** *Mobile business requires technical expertise spanning an unprecedented range of technologies. Choose a partner with the breadth and depth of expertise to match.*
- ***Pursue a business-driven approach.*** *Technology expertise is not enough, though. The security specialist needs to be able to understand your business model and match technical solutions accordingly.*

- ***The method counts.*** *How will you know if your company is in a safe pair of hands? Choose a partner that can demonstrate proven methods and processes for delivering e-business solutions as quickly and safely as possible.*
- ***One partner is better than ten vendors.*** *Trust is crucial. However, the more parties you involve, the more fragmented the solution and the greater the risks. If possible choose a single supplier that you can depend on to address all aspects of the project – technology, process and culture.*

Conclusion

Security is absolutely critical to the success of any mobile e-business. Even a relatively minor breach could undermine customer confidence and the reputation of your brand. This means companies need to fully understand and address the issues of security before they can realise the full opportunities of mobile e-business.

A number of technologies and solutions already exist that can form the basis of a wireless security architecture. The challenge now is to apply these to the new threats and risks of mobile e-business as part of a coherent strategy and process. Such a strategy will need to encompass an unprecedented range of channels, devices and parties. It will also need to address new areas related to security, such as how to exploit new location based services, while safeguarding consumer privacy.

Companies need to address all these issues before they deploy large-scale wireless services – and they will need to move quickly. First mover advantage is as applicable to wireless business models as it is to e-business in general. The race is on to develop the architectures, processes and organisational models that will deliver a flexible, end-to-end security strategy for mobile e-business.

About the author

Daniel Keely is the EMEA Wireless Security Competency Leader within the IBM Security and Privacy Services organisation. He leads a team of consultants responsible for business development, thought leadership and technical support related to the security of mobile e-business solutions. Daniel also practices as a Consultant, specialising in risk management. Before joining IBM (he joined in 1995) Daniel worked as a Systems Engineer for a Space and Military Systems company, where his responsibilities included the design, installation and testing of high security UNIX** and communication systems.

Acknowledgements

The author would like to particularly thank the following people for their help in producing this paper:

Michael Schnyder, Privacy Consultant, IBM Security and Privacy Services.

Mark Berkhoff, Security Architect, IBM Security and Privacy Services.

Trevor Hopkins, Technical Consultant, Wireless e-business services.

IBM United Kingdom Limited
emea marketing and publishing services (emaps)
Normandy House
PO Box 32
Bunnian Place
Basingstoke
RG21 7EJ
United Kingdom

The IBM home page can be found on the Internet at **ibm.com**

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program or service is not intended to imply that only IBM's product, program or service may be used. Any functionally equivalent product, program or service may be used instead.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

This publication is for general guidance only.