An onion ring framework for developing and assessing mobile commerce security

June Wei*

Department of Management and
Management Information Systems
College of Business, University of West Florida
Pensacola, Florida 32514, USA
E-mail: jwei@uwf.edu
*Corresponding author

Lai C. Liu and Kai S. Koong

Department of Computer Information Systems and
Quantitative Methods
College of Business Administration
The University of Texas-Pan American
Edinburg, Texas 78541, USA
E-mail: liul@utpa.edu E-mail: koongk@utpa.edu

Abstract: A five-layer 'onion ring' framework for analysing mobile commerce security requirements and for improving system security performance is presented in this research. Two quantifiable approaches, based on weighted scores applied to either a spider diagram or a decision solution matrix, are used to demonstrate how the security level can actually be objectively measured and evaluated in addition to the technical discussions on the framework's architecture.

Keywords: mobile commerce security; evaluation matrix; spider and relative weighted methods.

Reference to this paper should be made as follows: Wei, J., Liu, L.C. and Koong, K.S. (2006) 'An onion ring framework for developing and assessing mobile commerce security', *Int. J. Mobile Communications*, Vol. 4, No. 2, pp.128–142.

Biographical notes: June Wei is Assistant Professor in the Department of Management and Management Information Systems at the University of West Florida. She has published extensively and is an Editorial Board Member of the *Interdisciplinary Journal of Knowledge and Learning Objects*, *Journal of Information Privacy and Security, Interdisciplinary Journal of Information, Knowledge and Management*, and *International Journal of Mobile Learning and Organization*.

Lai C. Liu is Associate Professor of Computer Information Systems and Quantitative Methods at the University of Texas Pan American and is also a Fellow of the Computing and Information Technology Center. She has published extensively and is an Editorial Board Member of *E-Government* and *Interdisciplinary Journal of Knowledge and Learning Objects*.

Kai S. Koong is faculty member in the Department of Computer Information Systems and Quantitative Methods at the University of Texas-Pan American and is a Fellow and Associate Director of Economic Development of the Computing and Information Technology Center. He has published extensively and is an Editorial Board Member of *International Journal of Management and Enterprise Development*, *International Journal of Services and Standards*, *Journal of Computer Information Systems*, *International Journal of Information and Operations Management Education*, *Journal of Information Systems Education*, and *Journal of International Technology and Information Management*.

1 Introduction

Most people can now easily afford to own one, if not more, of the many varieties of available mobile devices. In addition to the traditional audio, text, and video features, many of the latest mobile devices can facilitate real-time business transactions around the globe. It is now common to see individuals, be they at an airport or on a ship in the open seas, engaged in communicative as well as collaborative activities with customers, suppliers, and partners with portable hand-held mobile devices. Given the popularity and technological advancements in these types of mobile devices, their future contributions and roles in the proliferation of internet commerce are expected to be critical.

However, just as mobile devices can be used to help businesses to facilitate commercial activities, they can also be used by perpetrators and criminals to victimise the same businesses. Such possibilities and threats are inherent in the basic characteristics of mobile commerce (m-commerce) because of its utilisation of any wireless device and some data connection to exchange information, services, or goods (Abuelyaman and Wen, 2004; Andreou *et al*., 2002). In operating terms, an m-commerce transaction is any type of transaction of an economic value which is conducted via a mobile device that uses a wireless telecommunications network with an e-commerce infrastructure (Tsalgatidou and Veijalainen, 2000). However, without a proven security infrastructure in their wireless communications, companies involved with internet commerce practices can very easily experience internal and external security breaches. All it takes is a fairly competent perpetrator and some innovative approaches to exploit the transmission processes and steal critical business intelligence from network devices.

Businesses have good reasons to be worried about the growing problem with online commerce security, particularly m-commerce. Each year, the increasing number of internet fraud cases reported by the Federal Trade Commission has indeed been alarming. Drawing from the dramatic increases in fraud reports in the recent few years, internet fraud is definitely expected to rise as the amount of commerce increases on the Net (Manuel, 1999). As online services are becoming more ubiquitous, the volume of m-commerce activity is expected to easily equal those of e-business. Put together, businesses should be seriously concerned on m-commerce security because perpetrators can now use the anonymous advantage of the internet to cause harm in real-time mode from anywhere on the globe. Worst of all, the victim or business can be harmed much more easily and quickly. It is even possible for the criminal to repeatedly harm the same

victim or business because the fraudulent electronic transactions can be repeatedly processed within a short period of time.

Given the types as well as amount of damages online perpetrators can cause to m-commerce, a major need and challenge for online commerce, at this time, is the development of new models and information systems that can secure resources from unauthorised access and prevent fraud (Olden, 2002). In particular, wireless systems that can secure networks and transmit reliable transactions in m-commerce have been identified as an area of priority by security software developers (Olla and Patel, 2003). Like all business practices, there is always a need for holistic models and evaluation approaches for assessing system effectiveness. Several researchers have examined the issue of computer security and m-commerce and proposed some noteworthy models and issues that are centered on security mechanisms and performance, environmental implementation issues, application requirements, and assessment of business key components. Some of these earlier studies and their contributions include:

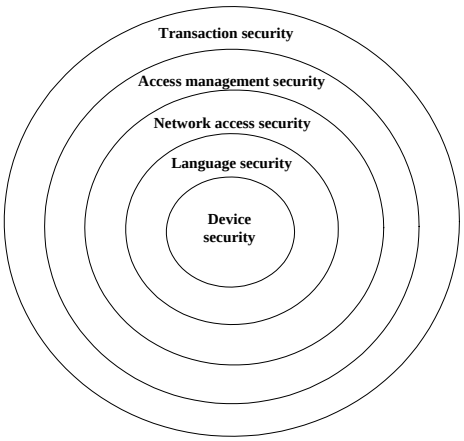
- Jansen and Karygiannis (1999) and their development of a mobile agent security system that can be used in mobile agent-based commerce applications such as contract negotiations, service brokering, auctions, and stock trading. Security requirements such as confidentiality, integrity, availability, and accountability are applied to this agent framework.
- Andreou *et al.* (2002) and their study on the performance of various mobile systems can confirm that mobile systems with lower security do allow their perpetrators to simply attack. For example, the radio wireless interface is one such device that is vulnerable to attacks. This is one good reason why wireless access should always include encryption, authentication, and other security mechanisms. The downside of this is the increase in complexity and delay in m-commerce transmissions.
- Vinaja (2002) and his three-dimensional framework can be used to identify security requirements for a specific mobile environment. The three dimensions include mobile users, mobile hardware, and mobile software. This framework is a useful beginning step to determine the specific implementation characteristics and needed security measures.
- Olla and Patel (2003) and their design of a context-aware mobile system which supports users with location-specific information servers and applications. The system uses the non-intrusive Push concept to deliver information to mobile users using cell-broadcast technology.
- Siau and Shen (2003) and their thoughtful discussions of the challenges of mobile communications and mobile services. Their contribution is inherent in the implications that were drawn from progress-to-date in technology as well as policy advancements.
- Yuan and Shang (2003) and the development of a framework to analyse m-commerce business models. Based on key business components, their taxonomy can be a useful model for businesses which need a systems approach to assess their operations.

While it can be agreed that the many noteworthy applications, models, and analyses identified in the research efforts indicated above have indeed been useful, studies that can address m-commerce security technical components, as well as application processes together, are still lacking. In addition, there is also a need for proven quantifiable approaches that m-commerce experts can actually use to assess effectiveness. This study is a pioneer effort aimed at addressing both those areas of need in the m-commerce security literature. First, this study will propose and validate an 'onion ring' framework that can logically link together all factors affecting m-commerce security performance. Second, two proven assessment methods are used to demonstrate how m-commerce security can be measured and evaluated. Finally, several suggestions are offered on where future research agendas of m-commerce security should be focused given the many incidences of internet fraud in the electronic marketplace.

2 The 'onion ring' m-commerce security framework

The notion of a multi-layer architecture for m-commerce security is definitely not a new one. The VAX/OS architecture is an excellent example of a popular operating software system which uses such an approach. Besides conceptual simplicity, the onion ring architecture offers excellent security by organising and matching access rights to increasing levels of responsibility and accountability. The research framework introduced in this paper classifies m-commerce security into five levels: mobile device security, m-commerce language security, wireless network access control security, m-commerce access management security, and m-commerce transaction security. This five-layer generic architecture was first applied to m-commerce security by Wei *et al*. (2003). In this study, technical specifications as well as application processes are added to explain how the proposed model can actually be developed. In addition, two assessment methods are used to demonstrate how the respective layers can be measured and evaluated. The key to understanding the success of the framework is inherent in the notion that protection needs to be in place in several layers. Each succeeding layer should also act as a kind of enclosure for the next layer thereby increasing effectiveness. This new multi-level framework to m-commerce security is depicted in Figure 1.

Figure 1 An 'onion ring' framework for m-commerce security



2.1 Layer 1: m-commerce device security

The root layer to enable m-commerce security is inherent in all the mobile communication devices because they can become a front-end security tool for m-commerce. Such devices may include, but are not limited to mobile phones, palmtops, handheld computers, and PDAs. For example, the integrated SIM card in mobile phones can be augmented using the private key digital signature of a Public Key Infrastructure (PKI) system. Wireless terminals can also act as security devices for gaining access into buildings by using the Global System for Mobile (GSM) part of the mobile phone or via an authentication mechanism called Bluetooth technology (May, 2002). Based on these front-end setups, the SIM cards can access the GSM network and identify the wireless device to the network. The smartcard operating system can be adapted to run on a SIM chip, which allows GSM communications phones to contain digital signatures and credit card numbers.

It should be pointed out here that the use of wireless devices to serve as front-end security devices is still at the infant stage of development. First, some of the more common operational uncertainties include altered information, denial of access, interrupted transactions, transmission delays, and power outage. Second, instances of modified electronic signature-signing programmes on mobile devices and stolen or modified smart cards have also been found to exist. Third, an attacker can distribute malicious code, cause denial of service, and reestablish connections without reauthentication due to intermittent service failures and unreliable conditions (Ghosh and Sawinatha, 2000). Fourth, determining where a hacker is from can be a relatively difficult task because an attacker can quickly get on or off-line and not be linked to any specific geographic location (Chess, 1998). Fifth, narrow bandwidth and capacity can force developers to give up security and encryption to simplify the process (Vinaja, 2002). Lastly, there is always the possibility for the loss of the wireless devices and the data in it.

While it is true that these uncertainties can be overwhelming, the good news is there are already some solutions that can be used to enhance security enforcement at this layer. Some of the proven methods include strict authentication protocols, cross-platform agent authentication mechanisms so the server can verify if the agent is coming from a trusted source, password authentication, smartcards or token authentication, and biometric authentication. At the receiving end, memory protection for processes, protected kernel rings, file access control, authentication of principals to resources, differentiated user and process privileges, sandboxes for untrusted code, and biometric authentication can be also added. Put together, this is why user authentication, merchant authentication, secure (encrypted) channels, user-friendly payment schemes supporting micro payments, receipt delivery, and simple user interfaces are critical in the design and development of mobile devices (Thanh, 2000).

2.2 M-commerce language security

The second layer concerns language security; that is, those elements dealing with m-commerce security system development. Proven security software applications and tested programme modules are the key to the successful functioning of this layer. The possibility of using a language where all programmes are safe is to develop a ‘safe’ language in which all codes have restricted access to operations that can affect

the environment. Such 'safe' language are Java and Telescript because they both use object-oriented programming languages to allow libraries to offer a secure interface to incoming code. Java also provides a byte-code verifier that can be utilised to check programmes at load time. The byte-code verifier assures an interpreter that a newly arrived piece of byte-code satisfies the same type-correctness properties that a correct compiler would enforce. At the machine level, a subset of language primitive operations can also be used to secure an incoming or untrusted piece of code (Farmer *et al*., 1996).

2.3 M-commerce network access control security

The third layer deals with wireless network access control security that provides access to m-commerce network access. In particular, the main function of this security layer is to restrict users accessing the wireless network. The good news is there are two existing technologies that can be used for security for this layer. For example:

1 GSM communication can provide a relatively secure connection through the PIN when turning on the handset and authentication protocol between handset and the network through Secure Sockets Layer (SSL) encryption of voice and data (Vihinen, 2004).

2 The smartcard is a better and preferred way of gaining access to a secure system. The smartcard can be in the form of a credit card or a SIM-like miniature card by using encryption to ensure confidentiality through a secure key. The key should be kept secret between the two parties. Two methods, symmetric and asymmetric, can be used to encrypt a document. In the symmetric method, the same key is used for encryption and decryption. However, the problem is that a third party could access the key during the transmission of a key to the recipient of the message. The asymmetric method is becoming more and more popular in m-commerce. It has two keys: a private and a public key. Information encrypted using the public key can only be retrieved using the corresponding private key, and the public keys of all users can be published in open directories, facilitating communications between all parties. Besides encryption, the public and private keys can also be used to create and verify digital signatures.

In addition to GSM and smartcards, it is critical that the wireless network solutions should have a Wireless Applications Protocol (WAP), a distinctive higher session security layer for mobile commerce transaction (Tan *et al*., 2003). WAP elements provide privacy, authentication/authorisation, integrity and non-repudiation. Specifically, in WAP, privacy is supported by Wireless Transport Layer Security (WTLS) Class 1 to encryption of mobile networks such as GSM. Authentication or authorisation is supported by WTLS Class 2 and Class 3. WAP Identity Module (WIM) in the mobile terminal can also provide an application-level security such as passwords/user names. Integrity and non-repudiation are provided by WTLS Class 1 via digital signature using WMLScript Crypto Library and WIM (Nokia, 2000).

Actually, WAP has undergone three evolutions: WAP 1.1, WAP 1.2, and next generation WAP. WAP 1.1 includes WTLS, a layer used for server authentication and data encryption. WAP 1.1 can provide confidentiality and integrity through WTLS Class 1, and WTLS server authentication through WTLS Class 2 (Nokia, 2000). WAP gateways can manage access to web servers, provide encryption through the WTLS

specification and authenticate users to enable a secure connection between the mobile device and the application server (Olden, 2002). WAP 1.2 can improve WAP security by using WIM and client/user certificates. WAP 1.2 provides WTLS client authentication through WTLS Class 3, and non-repudiation through WMLScript Crypto Library signText. WIM includes key pairs, certificates, and PIN numbers. WIM stores the private key securely in the mobile device, which can be used for client authentication, secure session handling, and digital signatures. All key operations are performed inside the WIM. WIM can be incorporated in a GSM phone's SIM (Subscriber Identity Module) smartcard to implement schemes such as SSL. Security is a key feature of SIM Application Toolkit (SAT) technology, since data confidentiality and integrity are already included in the SIM standard. WAP 1.2 also allows a WAP client to add a digital signature solution by adding SignText function to WMLscript. This is an alternative to the SIM-based signature solution used in digital signatures. The digital signature can then enable authentication of payments. WAP's next generation will provide end-to-end security via WAP gateway, WIM and client certificates, and WAP client's XHTML and WML browsers (Nokia, 2000).

2.4 M-commerce access management security

The function of the fourth layer is to control authorised resource access, audit a user's actions provide non-repudiation of transaction and access control for wireless web applications, and provide a scalable user administration model to support the much higher volume of mobile commerce users. In other words, there is a need for an application-level m-commerce access management system – once a user has been allowed to access a mobile commerce network, enterprises and services, – to:

- Control of resources that the user can access and the transactions he or she can execute
- Audit a user's actions to provide non-repudiation of transaction; provide access control for both web and wireless web applications from the same infrastructure so that the organisation can deploy and manage one security system for both m-commerce and e-commerce and provides a single point of control for setting, monitoring, and enforcing security policies
- Provide a scalable user administration model to support the much higher volume of m-commerce users
- Protect individual resources and control user access, such as the rule-based model, to eliminate the need for human intervention every time a user's profile changes
- Allow enterprises and service providers to delegate routine administration tasks such as adding, modifying and deleting users, changing passwords, and updating personal profiles
- Prevent fraudulent access in wireless applications through the real-time monitoring of business rule violations to track wireless web user activity (Olden, 2002).

Again, the good news is there are already a variety of proven technologies that can fulfill these functions. Multiple authentication methods, including PINs, passwords, WTLS mini certificates, and PKI, can control the resources and transactions that the user can

access and provide non-repudiation of transaction. Wireless PKI covers the infrastructure and the required procedures for trust provisioning in mobile transactions. PKI combines three aspects of security: authentication, confidentiality, and non-repudiation. Since mobile commerce architecture combines specialist authorities, digital certificate management systems, and directory facilities to create secure networks on top of unsecured networks, PKI can be used to enable authentication for servers and clients and digital signatures based on asymmetric cryptography (public and private keys); and to manage the keys, certificates, *etc*. Furthermore, wireless PKI infrastructure can be used to provide end-user friendly solutions, *i.e.*, user needs to remember and type only two PINs (authentication and digital signature) instead of several usernames and passwords and one-time password lists. An assumption here is the legal recognition of digital signatures will receive a broader support for digital certificates. If not, a credit card company can be held liable (May, 2002).

2.5 M-commerce transaction security

The fifth and last layer concerns m-commerce application level transaction security functions that secure sensitive data throughout the transmission, and logs all transactions. An application-level security system can achieve this by authenticating a user's identity, authorising the transaction, logging the transaction details and generating a digital receipt, and providing customers with detailed transaction reports.

3 Validation of the m-commerce security framework

As pointed out earlier, several noteworthy research works were used for the construction of the five-layer 'onion ring' topology in this study. Of particular importance to the development of the current framework include research by Andreou *et al* (2002), Farmer *et al*. (1996), Garfinkel (2002), Jansen and Karygiannis (1999), Norris (2001), Olden (2002), Tsalgatidou *et al*. (2000), Vinaja (2002) and Wei *et al*. (2003). These earlier research efforts were used because they provided the needed technical perspectives as well as process-oriented structures that are critical for validating the proposed construct.

A more practical perspective for the framework can be done by using the information system components as the base concept. Information system resources can also be defined as any organised combination of five components; *e.g.*, hardware, software, data, networks, and people. Together, these components gather, transform, and disseminate information in an organisation (O'Brien, 2002). People have to rely on information systems to communicate using physical devices (hardware), information processing instructions and procedures (software), communications channels (networks), and stored databases (data). Similarly, the m-commerce information systems that have these four non-human factor resource components will need to be protected by security measures to ensure their information quality and beneficial use, through which the business value of m-commerce security can be achieved (O'Brien, 2002). Table 1 illustrates how these five modules are interrelated to the resource components in information systems. The 'X' symbol means that the particular resource component has been covered in this framework. As can be seen in Table 1, the hardware resource is covered by the first

module (device) of this framework. The software component is covered by two modules (language and transaction). The network is covered by three modules (device, network access control, and access management), while the data is covered by four modules (device, network access control, access management and transaction). The people resource in information systems is required in all the five layers. Since these resources are mutually dependent on each other and encompass the earlier layers, it can be concluded that the proposed framework does have high theoretical construct validity.

Table 1 Comparisons of five layers in the framework with five resource components in information systems

Four components / *Five layers*	*Hardware*	*Software*	*Network*	*Data*	*People*
Device	X		X	X	X
Language		X			X
Network access control			X	X	X
Access management		X	X	X	X
Transaction				X	X

4 Assessment of the m-commerce security framework

In this study, two assessment methods are used to demonstrate how the m-commerce security framework proposed can actually be measured and evaluated. Both the methods are based on weighted performance scores that can be easily obtained from a variety of sources such as records in corporate archives or surveys of experts using a Delphi technique. The two examples are the spider-weighted and relative-weighted methods.

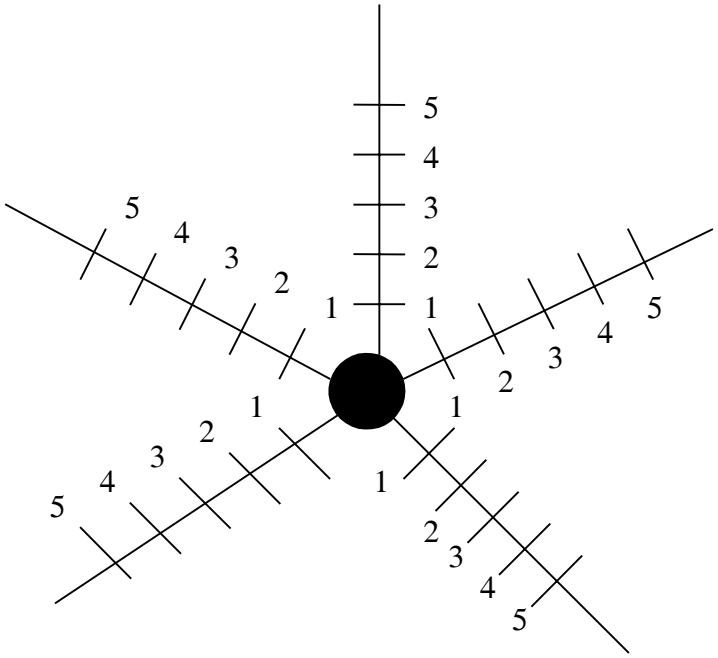
4.1 The spider-weighted assessment method

Based on the 5-S concept that originated in Japan, the spider-weighted method calls for regularly scoring each area within a facility on five characteristics related to good housekeeping and organisation of work space. Western companies have adapted and chosen their own meanings for implementing this assessment tool. For example, Boeing's version of the 5-Ss covers sorting, sweeping, simplifying, standardising, and self-discipline. The 5-S system usually entails public display of scoring against the 5-Ss. Some companies employ spider diagrams as the display device (Knod and Schonberger, 2001).

Similarly, in the first assessment example here, a spider diagram is also used as the display device (M) of the proposed model. The raw diagram has five arms that extends outward from a central point. Each arm representing one of the M's has a scale from zero to five points. A five at the outer boundary for each arm is the target for perfect security. A designated outside rater can be asked to rate each unit. The rater could be a higher-level manager, a quality engineer, or security manager. When the scores or dots are connected to the arms, the rater will find a simple web. The larger the web, the closer it is to the five points at the outer boundary. Incidentally, along with the discipline of

rating the Ms, it is often a good idea to dedicate certain people as responsible for rating certain security layers. Figure 2 illustrated the M's spider diagram displaying scores against the five M's.

Figure 2 Spider diagram displaying scores against the five M's



Once the layers and the ratings have been identified, the next step is to assess the m-commerce security of the system. To that end, a weighted measuring method can be developed to measure the respective m-commerce security levels. Given the five layers, the complete formula can be simply stated as:

$$SL = \Sigma_{i=1}^{5} W_i * S_i$$

where *SL* is the security level of the m-commerce system.

This cumulative score is the summation of each individual layer's security level. Such a security level can be measured by multiplying the security weight of the *i*th layer (W_i) with the security scale of that particular layer (S_i). It is important to note that the weight of the *i*th layer (W_i) may vary among m-commerce systems because those numbers are based on the arbitrarily selected importance level given by experts or managers which satisfies the criteria $\Sigma_{i=1}^{5} W_i = 1$. The scale of individual layer's security (S_i) can be measured by asking the subject matter experts to answer some five-scale measurement question such as:

Question: To what extent is security mechanism developed on this layer for m-commerce?				
1	2	3	4	5
none or very little	little	moderately	much	very much

where:

1 – none or very little (security mechanism is not developed at all) at this layer
5 – very much (security mechanism is fully developed) at this layer.

4.2 The relative-weighted assessment method

The systematic rating method has been used successfully in the area of location evaluation in facility design (Knod and Schonberger, 2001). This method could also be used to evaluate m-commerce system security. A good systematic rating method – on m-commerce security with weights – is expected to contain three important steps.

The first step is to comparatively rate the importance of the respective security factors. Each factor should be compared with all others. For example, the importance of the factors can be rated using a four-point scale (4 – major preference; 3 – medium preference; 2 – minor preference; and 1 – little/no preference). The rating is then inserted in the matrix in Figure 3. In this case, the intersection of B and C is rated in the diamond-shape box 3C. By checking that cell, a three means the factor has a medium importance preference, that is, a medium importance preference of C compared to B. The bottom row contains the total weighted raw scores for each factor that is obtained by adding the number of times each letter appears in the matrix.

Figure 3 Evaluation matrix for relative weighting of security factors

Factors					
A Device security	**3A**	**A/C**	**2A**	**A/E**	
B Language security	**3C**	**B/D**	**2E**		
C Network access security	**2C**	**2E**			
D Access management security	**D/E**				
E Transaction security					
Factor letter	**A**	**B**	**C**	**D**	**E**
Total weighted raw score	7	1	6	2	6

Importance

4 – major preference

3 – medium preference

2 – minor preference

1 – (letter/letter) no preference, each scores one point

In Step 2, the object is to rate the m-commerce security under consideration against the security factors. Table 2 is an example of a matrix that shows the system ratings on a ten-point scale for three systems. As in the previous case with the previous methods, those scores can be easily obtained from a variety of sources such as records contained in corporate archives or by surveys of expert using a Delphi technique. As in the case of this example, System 1 received the highest rating, a ten on Factor A device security. Other scores attained by the respective factors are also demonstrated on the matrix. However, all the ratings in this table should not be accepted as the final ratings. A third and final stage is needed.

Table 2 Rating prospective m-commerce security

	System		
Factors	*1*	*2*	*3*
A Device security	10	6	4
B Language security	3	5	6
C Network access security	8	7	9
D Access management security	6	7	10
E Transaction security	6	8	6

In the third and final matrix, the total weights for each factor from the first step (Figure 1) and the second step (Table 2) are combined to obtain the total weighted scores for each factor and rankings. In the sample matrix computed and shown of Table 3, System 1 has ten points for device security and device security was rated with a seven in importance. Therefore, $10 \times 7 = 70$ and this total is displayed in the upper-left corner in Table 3. The rest of the matrix is computed by repeating the same process. When all the scores are computed, the column totals are added and the total weighted scores are compared. In this case, System 1 is the preferred choice with 169 points even though the difference between Systems 2 and 3 is not that great.

Table 3 Weighted security scores

	System		
Factors	*1*	*2*	*3*
A Device security (7)	70	42	28
B Language security (1)	3	5	6
C Network access security (6)	48	42	54
D Access management security (2)	12	14	20
E Transaction security (6)	36	48	36
Total weighted score	169	151	144
Ranking	1	2	3

5 Summary, conclusion and implication for future research

This study presented a variety of logical layers as well as their associated technical components that can be used for the development of a multi-layer m-commerce security model called an 'onion ring' m-commerce security framework based on the VAX/OS architecture and a variety of noteworthy research. The strength of this model is inherent in its ability to logically link all factors affecting m-commerce security performance together to systems components.

The five m-commerce layers identified and discussed are related to devices, language, wireless network access, access management and transaction requirements. This framework can assist m-commerce system experts to better analyse and (re)design to increase security performance. In addition to its usefulness for specific mobile environments that can be based on the five dimensions in the 'onion ring' framework, this may also be utilised to determine specific analysis, design, and implementation characteristics by estimating all aspects of security performance in mobile commerce.

Two methods were used to demonstrate how the framework can be measured and evaluated. Based on the 5-S concept, the spider-weighted method is simpler to use and can provide a more visual analysis of the system. The second method, the relative-weighted method, is a more systematic analysis that requires the collection of more data. However, the second method may be more valuable to security managers because it reduces data which could be used to influence the final decision. Best of all, both the two measurements are scalable. More factors could be added and if needed, one factor can also be split into more subfactors.

Beyond the need for more practical, holistic, models that can be assessed, the goal of attaining a reasonably secured m-commerce security environment may still be quite a distance away. Part of the problem with m-commerce security is there are always new techniques and innovative approaches devised by perpetrators to cause malicious mischief and by criminals to steal. Apart from the constant need for new devices and techniques, there are at least five main areas where research is critically needed, namely:

1 *Usability*

   This involves the development of a security scheme that remains convenient and simple to use. Normally, encryption is the way to establish a secure transmission. However, even the strongest encryption methods require authentication via a digital certificate to protect the next generation of m-commerce transactions. Unfortunately, digital certificates take time to transmit because the bandwidth may be unacceptable in a wireless transmission environment. Therefore, creating a more simple and wireless-friendly digital certificate is of tremendous importance at this time.

2 *Integrated security solutions*

   Integrated security solutions are important in mobile commerce because they increase reliability and decrease the need for bandwidth consuming add-on cryptographic software. For example, the mobile phone with its integrated SIM card is a good solution for the private key digital signature of a PKI system. Such innovative solutions are needed.

3 *Increase bandwidth and capacity limitation*

Due to bandwidth and capacity limitation, some m-commerce developments have not been able to implement security functionality. Third generation (3G) wireless solutions are needed to address these two limitations.

4 *Reusable m-commerce security framework*

As it is in the programming world, development of reusable frameworks can help hasten the security industry reaction time to new challenges. The five layers presented in this paper may be a good starting point for the development of the next generation of m-commerce security systems, be they tools or methods.

5 *M-commerce security system evaluation*

Evaluation of effectiveness is always a critical function in all systems. Other evaluation systems that can measure the security levels of m-commerce systems – especially those that can pinpoint weaknesses throughout the transmission process – will be helpful.

Acknowledgements

An earlier version of this paper was presented at the International Conference of Pacific RIM Management that was held in Seattle in 2003. Partial funding for the earlier version was provided by a grant from the Department of Education to the Computing and Information Technology Center at the University of Texas – Pan American. The revisions and expansions contained in this new paper are supported by a Creative and Scholarly Research Activity Grant at the University of West Florida that was allocated in 2004.

References

Abuelyaman, E. and Wen, H.J. (2004) 'An efficient wireless transmission method for m-commerce', *International Journal of Mobile Communications*, Vol. 2, No. 4, pp.405–417.

Andreou, A.S., Chrysostomou, C., Leonidou, C., Mavromoustakos, S. and Pitsillides, A. (2002) *Mobile Commerce Applications and Services: A Design and Development Approach*, Retrieved from the World Wide Web, pp.1–9, http://www.mobiforum.org/proceedings/papers/02/2.2.pdf

Chess, D.M. (1998) 'Security issues in mobile code systems', in G. Vigna (Ed.) *Mobile Agents and Security*, Springer.

Farmer, W.M., Guttman, J.D. and Sarup, V. (1996) *Security of Mobile Agents: Issues and Requirements*, Retrieved from the World Wide Web http://csrc.nist.gov/nissc/1996papers/NISSC96/paper033

Garfinkel, S. (2002) *Web Security, Privacy and Commerce*, 2nd edition, CA: O'Reilly & Associates, Inc.

Ghosh, A.K. and Sawinatha, T.M. (2000) 'Software security and privacy risks in mobile e-commerce', *Communications of the ACM*, February, Vol. 44, No. 2, pp.51–57.

Jansen, W. and Karygiannis, T. (1999) *Mobile Agent Security*, MD: US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Knod, E. and Schonberger, R. (2001) *Operations Management: Meeting Customers' Demands*, New York: McGraw-Hill Higher Education.

Manuel, C. (1999) *Internet Fraud Watch*, February, Retrieved from the World Wide Web http://www.fraud.org./internet/9923stat.htm

May, P. (2002) *Mobile Commerce: Opportunities, Applications, and Technologies of Wireless Business*, United Kingdom: Cambridge University Press.

Nokia (2000) *Security in Mobile Transactions*, Retrieved from the World Wide Web http://www.nokia.com

Norris, M. (2001) *Mobile IP Technology for M-Business*, MA: Artech House, Inc.

O'Brien, J. (2002) *Management Information Systems: Managing Information Technology in the E-Business Enterprise*, New York: McGraw-Hill Companies, Inc.

Olden, E. (2002) *Securing m-Commerce*, Retrieved from the World Wide Web http://e-serv.ebizq.net/mob/olden_1. html

Olla, P. and Patel, N.V. (2003) 'A framework for delivering secure mobile location information', *International Journal of Mobile Communications*, Vol. 1, No. 3, pp.289–300.

Siau, K. and Shen, Z. (2003) 'Mobile communications and mobile services', *International Journal of Mobile Communications*, Vol. 1, No. 3, pp.3–14.

Tan, J., Wen, H.J. and Gyires, T. (2003) 'M-commerce security: the impact of Wireless Application Protocol (WAP) security services on e-business and e-health solutions', *International Journal of Mobile Communications*, Vol. 1, No. 4, pp.409–424.

Thanh, D.V. (2000) 'Security issues in mobile commerce', *Proceedings of the 1st International Conference on Electronic Conference and Web Technologies (EC-Web 2000)*, London, pp.412–425.

Tsalgatidou, A. and Veijalainen, J. (2000) 'Mobile electronic commerce: emerging issues', *Proceedings of the 1st International Conference on Electronic Commerce and Web Technologies (EC-WEB 2000)*, London, pp.477–486.

Tsalgatidou, A., Veijalainen, J. and Pitoura, E. (2000) 'Challenges in mobile electronic commerce', *Proceedings of IEC 2000, 3rd International Conference on Innovation Through e-Commerce*, Manchester, UK, pp.14–16.

Vihinen, J. (2004) 'Identifying the limitations and capabilities of m-commerce services in GSM networks', *International Journal of Mobile Communications*, Vol. 2, No. 4, pp.329–342.

Vinaja, B.R. (2002) 'A three-dimensional framework for security implementation in mobile environments', in J.H.P. Eloff *et al*. (Eds.) *Advances in Information Security Management and Small System Security*, Kluwer Academic Publishers, pp.35–43.

Wei, J., Liu, L.C. and Koong, K.S. (2003) 'A framework for delivering mobile commerce security system', *Proceeding of International Conference on Pacific Rim Management*, Seattle, Washington.

Yuan, Y. and Zhang, J. (2003) 'Towards an appropriate business model for m-commerce', *International Journal of Mobile Communications*, Vol. 1, Nos. 1–2, pp.35–56.