2008

A Risk Assessment Framework for Mobile Payments

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra,U.N.S.W. Sydney, A.N.U. Canberra, University of Hong Kong,
roger.clarke@xamax.com.au

21st Bled eConference
eCollaboration:
Overcoming Boundaries through Multi-Channel Interaction
June 15 - 18, 2008; Bled, Slovenia

A Risk Assessment Framework for Mobile Payments

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra
Visiting Professor at U.N.S.W. Sydney, A.N.U. Canberra,
and the University of Hong Kong
Roger.Clarke@xamax.com.au

Abstract

Progress in Mobile Commerce is heavily dependent upon effective and reliable payment mechanisms. Security concerns loom as a major impediment to widespread and rapid adoption, and there is accordingly an urgent need for a framework within which security issues in mobile commerce can be evaluated. This paper draws on lessons from prior payment mechanisms in order to present such a framework. It provides insights into the use of the framework by performing a test application. Implications for policy, practice and research are drawn.

Keywords: M-Commerce, wireless, payment schemes, security, malware

Introduction

A variety of mobile technologies and mobile services have emerged during the last two decades. The term M-Commerce was adopted by marketers in the late 1990s, and predictions were made of rapid growth in the volume of commerce conducted through mobile devices. Recklies (2001) reported a Boston Consulting Group prediction that "global M-Commerce sales" would rise rapidly to $20bn in 2001, $60bn in 2002 and $100bn in 2003. The guesses of other consultants were wildly different. For example, Vrechopoulos et al. (2002) said that "According to Jupiter Research (2001), the global m-commerce revenues will reach $22.2 billion in 2005". See also ePayNews.com (2002).

By 2004, Jupiter Research had become vastly more optimistic, offering "Global mCommerce Revenue Projections for 2009" of $426 billion, most of it in "phone-based retail POS sales" ePayNews.com (2002). On the other hand, the slow growth had led other organisations to offer much more circumspect prognostications, e.g. "2006 will continue to see the development of experiential mobile applications and the emergence of m-commerce services, increasing in reach and importance over the next two years" (Atos 2005, p. 12). Juniper Research remains unabashed, and was quoted in early 2008 as forecasting that "over 612 million mobile phone users would generate over $US587 billion ... worth of financial transactions by 2011" (Moses 2008).

Despite one or two consultancy groups' wild enthusiasm, the growth of M-Commerce has a very patchy record. One major concern is that the risk of financial loss acts as an impediment to the adoption of mobile commerce. This may be because of widespread knowledge of actual losses, or reports of vulnerabilities, or just from uninformed concerns and natural risk-aversion. In order to

understand the substance of the issue, and to avoid unnecessary delays in mobile service adoption, it is highly advisable that payment schemes intended for use in mobile contexts be subjected to risk assessment.

As with any form of trading, M-Commerce involves multiple steps, including partner discovery, information exchange, negotiation, contracting, delivery and settlement. The settlement step necessitates considerably greater care than the others, because the payments process creates considerable opportunities for funds to be stolen, with low likelihood of the thief being apprehended or the proceeds recovered, and with the possibility that the victim may not even be aware that the theft has occurred.

The term 'mobile payments' is used in this paper to refer to any payment that is conducted by means of a mobile access device and wireless network connection. By 'mobile access device' is meant 'any device that provides users with the capacity to participate in transactions with adjacent and remote devices by wireless means'. Such devices comprise at least a processor, systems software, application software and wireless communications capability. They are commonly also capable of at least some forms of physical interaction with one or more storage devices such as magnetic disks, CDs, DVDs, and solid-state tools (e.g. 'thumb drives' or 'memory sticks' or, currently, 'USB sticks').

In 2008, relevant mobile access devices fall into the following categories:

- mobile telephones;
- handheld computing devices. These are numerous and diverse, and include personal digital assistants (PDAs) of various kinds, games machines, music-players like the iPod, and 'converged' / multi-function devices such as the Apple iPhone;
- wearable computing devices, such as watches, finger-rings, key-rings, glasses, necklaces, bracelets, anklets and body-piercings;
- processing capabilities housed in other, generally much smaller packages (or 'form factors'), such as credit-cards and RFID tags. Subcutaneous or embedded chips are emergent, and may need to be treated as 'wearable' or as a separate category.

In general, transactions from desktops and portable PCs are excluded from this analysis, even if conducted over a wireless network connection. It may, however, be appropriate to include within the scope the nomadic use of portables, e.g. transactions conducted on the move, in aircraft, trains and cars.

Relevant transmission means include:

- cellular networks that were originally designed for mobile phones and that have had data transmission capabilities added, such as GSM/GPRS, CDMA and W-CDMA;
- wide-area and local area networks that were designed for data transmission, including both standards-based approaches such as 'WiFi'/IEEE 802.11x and 'Wimax'/IEEE 802.16 and proprietary protocols such as iBurst; and
- other forms of wireless communication, such as infra-red links and the related techniques used by contactless cards, radio frequency identification (RFID) tags and near field communications (NFC).

Mobile payments using such devices over such networks may be made in a variety of circumstances (Pousttchi 2003), including:

- MCommerce itself (e.g. the purchase of content, such as location-specific data and audio and video streams);
- the purchase of goods and services in conventional eCommerce in both Business-to-Consumer (B2C) and Business-to-Business (B2B) patterns;
- the purchase of goods and services at conventional points of sale; and
- consumer-to-consumer (C2C) transactions involving transfers of value between individuals.

A considerable technical literature exists, but it is characterised by enthusiasm and narrow focus. Typical of the approach adopted is Herzberg (2003), which focusses on the links and flows between providers, and makes unjustified assumptions about the links and flows between users' devices and providers. Many of the infrastructural features assumed in this literature have not been deployed, or have been deployed but not adopted. In addition, industry coalitions have published technical specifications, such as MPF (2006). But these lack clear requirements statements against which specific designs and implementations can be assessed.

In a survey of papers published in the IS literature between January 2000 and September 2004, Scornavacca et al. (2005) found only 4 of 253 articles that addressed security. By the end of 2007, the specialist M-Business literature index at Scornavacca (2007) contained over 1,100 references, of which 30 had 'security' in the title, 33 had 'payment' in the title, but only one had both (Linck et al. 2006). Dahlberg et al. (2007) identified three that "discussed technologies in terms of m-payment security", three that "proposed new tools or mechanisms to improve security", and a further four papers of an empirical nature that dealt with security topics. Lee et al. (2004) includes several chapters on the security of mobile transactions. A limited amount of attention has also been paid to it in adjacent literatures, e.g. Choi et al. (2006).

Many authors have considered mobile payments from a technical perspective, but far less attention has been paid to practical application, security aspects, and acceptability by the users of mobile devices. See, however, Rawson (2002) which considered legal aspects of mobile transactions, Pousttchi (2003) and Kreyer et al. (2003) which discussed security as one among many factors in the adoption of mobile commerce, and Zmijewska (2005). Based on an empirical study, van der Heijden H. (2002) found that "security was emphasized, both for merchants and for consumers, but it was usually framed in a factor that can best be described as 'perceived risk'". Misra & Wickramasinghe (2004) proposed a 'trust model' for mobile commerce generally.

The purpose of this paper is to present a framework within which risk assessment of mobile payment arrangements can be undertaken. It commences by reviewing the experiences of payment mechanisms that have been used both prior to the emergence of open, public networks and more recently. This provides a basis on which a framework can be developed which reflects the technical and commercial infrastructure, and the relevant categories of harm, threats, vulnerabilities and safeguards. A report is provided of a small test application of the framework. Implications are drawn for policy, practice and research.

Lessons from Existing Payment Mechanisms

A rich set of payment mechanisms exists, reflecting the enormously varied circumstances in which people and organisations conduct transfers of value. The designs of these mechanisms also reflect the risks that the circumstances embody. It is strongly advisable that mobile payment schemes take into account the accumulated knowledge about risks and risk management. Appendix A to this paper (accessible at a URL provided below) accordingly provides a brief catalogue of payment mechanisms. This section draws some inferences from it that are of significance for the security of mobile payments.

A breakthrough application in the use of large-scale data networks was Automated Teller Machines (ATMs, called by various names in various countries), which became widespread during the early 1980s. ATMs are not a payment mechanism in themselves, because their primary and still dominant usage is for the withdrawal of cash. They are important to the discussion for two reasons.

The first is that they embodied a relatively quite robust security design. They involve two-factor identification ('have' a card and 'know' the PIN); the PIN is keyed in a manner that makes observation reasonably difficult; the design ensures that the PIN is not accessible outside the secure PIN-pad and/or a secure device on the financial institution's premises; and hence the authenticator is protected from both physical and electronic observation.

The second reason ATMs are important is that they paved the way for EFTPOS schemes (Electronic Funds Transfer at Point of Sale). These automated the capture and validation of debit-card transactions at merchants' points of sale, resulting in charges against the account-holder's deposit with their financial institution (Clarke & Walters 1989, Clarke 1990, 1992). Debit EFTPOS embodied similarly strong security features to those used in ATM systems.

The scope of EFTPOS was rapidly extended to the capture of credit-card transactions. This used far less secure arrangements, however, because no PIN was required. The primary purpose was the transfer of data capture costs to the merchant. The security improvements were largely limited to the automation of processes for checking stop-lists of cancelled credit-card numbers – although the lists may as a result be somewhat less out-of-date.

ATM and EFTPOS networks are closed, and people's interactions with them are tightly controlled. The same is not true of the open, public Internet that became available from about 1993 and that ushered in what is now commonly referred to as the 'Wired' era. Key differences were:

- users' own devices were now directly connected with the technological infrastructure;
- the infrastructure offered a very wide range of services. But payments were not originally among them, and were grafted on;
- basic Internet infrastructure embodied essentially no security features;
- during the period from 1993 to the present, users' desktop and portable access devices have become increasingly powerful;
- a wired connection is commonly in a fixed location and a setting that has some formality about it and in most cases freedom from excessive noise and distracting activity (e.g. work, home office, library, airport lounge, 'Internet café');
- the technical awareness of users was and continues to be highly varied;
- the commercial astuteness and wariness of users also was and continues to be highly varied.

With closed payment systems, transactions at point-of-sale required presentation of the card, and production of a signature that could be matched against the previously-recorded signature on the back of the card; whereas in Mail-Order-Telephone-Order (MOTO) / Card-Not-Present transactions that safeguard was completely missing.

The use of credit-cards on the Internet adopted the MOTO model, and hence two-factor authentication was reduced to single-factor, because there is no requirement that the payer demonstrate that they 'know a secret'. Moreover, the 'have' factor is reduced from 'have the card' to 'have the details recorded on the card'. The MOTO model, as applied to Wired-Era Payments, is based on the pretence that credit-card details are in some way protected. It relies on:

- levels of honesty in the community being and remaining at a high level;
- consumers reconciling their accounts, doing so promptly, and discovering and reporting entries that appear to them to be spurious (because the front-line bearer of financial risk is consumers who fail to do so); and
- self-insurance by merchants (who bear the remainder of the financial losses arising from errors and fraud, because banks issue 'chargebacks' to their accounts).

An attempt was made during the late 1990s to impose stronger safeguards. The Secure Electronic Transactions (SET) initiative involved three-way authentication, but foundered in the marketplace (see for example Clarke 1996b). Since 2000, another attempt is being made, in the form of 3-D Secure, a Visa initiative branded as 'Verified by Visa', and cross-licensed to MasterCard as SecureCode' and to JCB as J/Secure (Visa 2008). It requires some kind of authentication of the payer's claim to be the cardholder; but it does not specify what form authentication should take, and adoption has been slow.

Internet Banking involves an account-holder with a financial services organisation conducting transactions on their account from an Internet-connected device. It took some years to emerge as a reliable and accepted service, to a considerable extent because of the need for a security design with at least the same level of robustness as ATMs and debit-card transactions via EFTPOS

terminals. The threat profiles change rapidly, and safeguards are in a state of flux. Conventional two-factor authentication is increasingly considered to be inadequate, because the PIN is keyed into an insecure key-pad on an insecure access device. Three-factor schemes are being increasingly implemented. These commonly feature one-time passwords extracted from an electronic token (often carried on a key-ring) or delivered through an 'out of band' channel such as an SMS message.

Debit transactions over the Internet are emerging as an extension to Internet Banking. For example, the Canadian Interac Online service re-directs the payer to their bank, and the payment instruction is captured within the bank's Internet Banking environment. This leverages well-trusted infrastructure, but requires careful interfacing between the web-based applications of very large number of merchants and moderate numbers of financial services organisations.
The transition into the 'Unwired' / M-Commerce era brings with it further changes. These include:

- a less powerful access device, in many cases running minimalist or stripped-down systems software. See Grand (2004);
- unwired connection, and hence variable locations and informal contexts of use, many of them subject to ambient noise and many distractions competing for the user's attention;
- many technically-unaware users, whose mode of use is casual, hurried and unconsidered;
- many users who are not commercially-astute or wary, who are strongly oriented towards convenience, fashion and entertainment, and who behave as though they were not averse to financial risk.

A particular characteristic of payment schemes that is often overlooked is the question of the identifiability of the parties. Barter and cash payment systems are inherently anonymous (although of course other aspects of the transaction may identify either or both transacting parties). Most other payment mechanisms carry at least some form of identifier, which may enable the transaction to be associated with a particular natural or legal person. The parties may, however, be pseudonymous, if there are significant barriers to be overcome in order to establish the association. Electronic payment mechanisms have the potential to generate a comprehensive and intensive record of a person's transactions, and even of the person's movements. Designers who fail to reflect the interests of payees, and particularly payers, in avoiding the creation of such dangerous data, create impediments to adoption.

As credit-card transactions migrate into the mobile context, all of the issues with MOTO transactions arise, and are joined by additional threats and vulnerabilities. The much more responsible approaches involving Internet Banking, debit-card transactions linked to Internet Banking and even credit-card transactions with authentication, are not as severely deficient, but they still involve additional risks when used in a mobile context. The framework proposed below reflects lessons such as these, that have been learnt from prior payment mechanisms.

The Framework

This section expresses a framework intended to assist in defining and addressing the risk profiles of the unwired payment mechanisms that underpin M-Commerce. Risk assessment is an established business process, and is described in text-books (e.g. Peltier 2005, Landoll 2005, Slay & Koronios 2006) and industry standards (e.g. AS/NZS 3931-1998, AS/NZS 4360-1999 and the long-promised ISO 27005 standard that is currently scheduled to emerge in 2009 to complement the foundation Information Security Management Systems standards ISO 27001 and 27002).

In order to perform a risk assessment, it is necessary to establish a sufficiently deep appreciation of a range of aspects of the relevant infrastructure, processes and contexts. The framework proposed here reflects the 'trust model' of Misra & Wickramasinghe (2004), but it is more comprehensive, and is specifically focussed on payments. The framework comprises the following dimensions, which are represented in diagrammatic form in Exhibit 1:

- a security model that reflects conventional risk management approaches (section 3.1);

- a technical architecture model whose purpose is to encompass all elements of the infrastructure on which mobile payments depend (section 3.2);
- a commercial architecture model that identifies the actors that may be involved in mobile payments, together with their interests (section 3.3);
- a transaction process model that shows the flows at a sufficient level of detail to enable security analysis (section 3.4);
- checklists of harm, threat, vulnerabilities and safeguards that may be relevant to the assessment of risk in any particular mobile payment context (sections 3.5, 3.6 and 3.7).

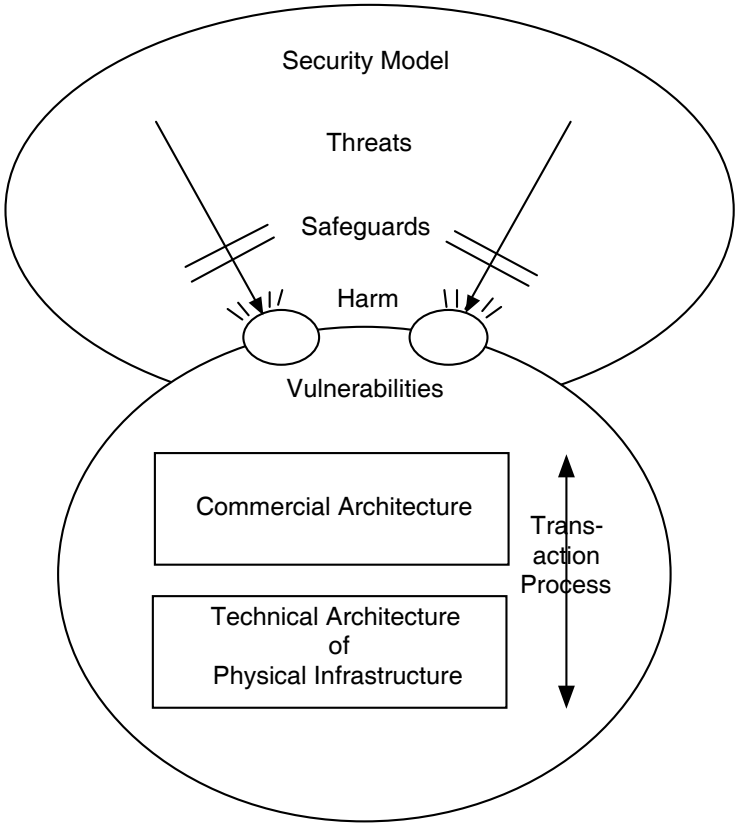

***Exhibit 1**: A Risk Assessment Framework for Mobile Payments*

The Security Model

The conventional computer security model is adopted in this paper (e.g. Clarke 2001a, OECD 2002, ISO 2005). Under this model, threatening events impinge on vulnerabilities to cause harm. Safeguards are used in an endeavour to protect against threats and overcome vulnerabilities, in order to deter, prevent, detect, investigate or ameliorate the events or the harm. Security is a condition in which harm does not arise, because threats and vulnerabilities are countered by safeguards. For a fuller exposition, see Appendix B, Clarke (2001a) and standard texts in the area.

The Technical Architecture Aspect

The purpose of the technical architecture model is to identify the physical locations and components and the inter-relationships among them, which together make up the relevant technical infrastructure. Because of the considerable diversity in mobile services, a single definitive model

is not feasible. This section accordingly sets out to provide a comprehensive catalogue of elements, supported by an indicative diagram in Exhibit 2.

The relevant infrastructural elements are as follows:

- a human user;
- the user's physical context while conducting a transaction;
- an access device;
- possibly a personal area network (such as Bluetooth), and a personal intermediary node (at proxy, router and/or lower levels);
- transacting devices, such as smartcard-readers, and readers of RFID and NFC communications, which conduct transactions with access devices;
- access networks (whether local or wide-area) – which by definition comprise unwired infrastructure – including Internet Access Providers (IAPs) to provide transacting devices with means of interacting with remote devices over the Internet, and intermediating base stations, wireless routers and possibly proxy-servers;
- core networks, which are commonly wired although they could in principle be unwired as well, including backbone routers and proxy-servers;
- host devices which run server software and hence provide various kinds of services, necessarily including payment services, but possibly also payment intermediary services.

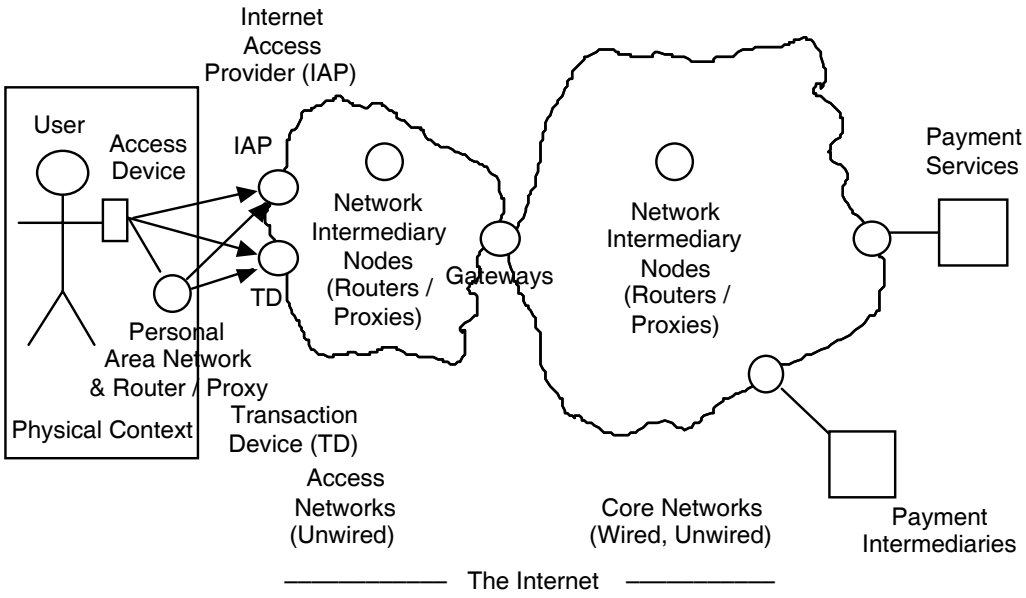

***Exhibit 2**: An Indicative Technical Architecture Model*

The Commercial Architecture Aspect

The purpose of the commercial architecture model is to identify the relevant categories of natural and legal persons, their interests, the interactions among them, and their legal rights and duties, particularly those arising under commercial law including contract.

According to Slay & Koronios (2006), the Internet Online Trading Protocol (IOTP) framework classifies five roles: customer (i.e. payer), seller (i.e. payee), payment handler, delivery handler and customer support.

However, this is too limited for the more complex patterns that are already evident in Internet payment systems. Many more categories of actors are directly involved, including Internet access

providers, carriage service providers, commercial intermediaries (such as Paypal), transaction service providers (such as banks and credit-card companies), and payment services providers (such as deposit-holders, lenders and insurers). Yet more actors may need to be considered, such as regulators, complaints bodies such as financial services ombudsmen, and consumer rights representative and advocacy organisations. Moreover, consumers may need to be segmented rather than treated as a single category, e.g. to separate out the particular interests of the mobility-disadvantaged and the sight-impaired, and to reflect the needs of people with limited financial assets, particularly those who have no credit-card.

When undertaking a risk assessment, a clear understanding is needed of the laws, policies and practices that apply to the categories of mobile transaction under consideration. The study may need to extend across multiple jurisdictions.

In some circumstances, there may also be a need to allow for the organisational context within which the access device is used. Employers may see it as being to their advantage to assist their employees to protect themselves, because they are very likely to conduct company and personal business on the same device. Support of a similar kind may be available from computer clubs, and may be able to be acquired from suppliers of consumer devices and related services, perhaps as an extension to the basic services package. Locations that make network connections available for free or for fee (such as libraries, Internet cafés, and coffee-shops that operate Wifi 'hot-spots') may provide protections. On the other hand, the access networks in such locations may lack protections that the consumer might assume to be in place; and they may even be set up by the operator or a third party to create opportunities for mis-deeds.

The Editor of the specialist journal Computing & Security commented in May 2007, that "Mobile computing presents serious security challenges in part because mobile workers are physically removed from the immediate control of organizations' security staff. ... Furthermore, many security controls that are in effect when users connect to an organization's network from a location within the workplace are not likely to be in effect when users engage in mobile computing while on travel or at home. ... Mobile users also create new entry points into networks. ... When risks related to “shoulder surfing” are also taken into account, it is impossible to conclude anything else but that mobile computing is becoming downright dangerous" (Schultz 2007).

The Transaction Process Aspect

In order to undertake a risk assessment of a mobile payment service, it is essential that a sufficient appreciation be gained of the mechanisms involved. A wide variety of modelling formalisms is available. An example of a simple overview diagram is in Exhibit 3.

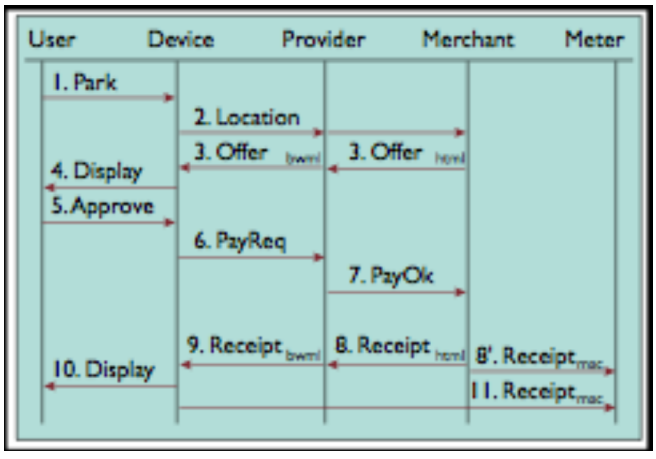

***Exhibit 3**: A Sample Process Flow – from Herzberg (2003), p. 56*

A diagram of this nature has the advantage of enabling easy cross-referencing with the commercial architecture considered in the previous section. Commonly, there will be a need for both an overview of that nature and more detailed models, whether modelled using tools associated with procedure-oriented flowcharts, structured analysis and design such as Yourdon & deMarco or Gane & Sarson Data Flow Diagrams (DFDs), or object-oriented forms.

The Harm Aspect

Generically, categories of harm include:

- injury to persons;
- damage to property;
- financial loss;
- loss of value of an asset;
- breach of personal data security, or privacy more generally;
- inconvenience and consequential costs arising from identity fraud;
- serious inconvenience and consequential costs arising from identity theft; and
- loss of reputation and confidence.

In the current context, it is appropriate for the harm model to focus primarily on financial loss to users, and (under the commercial arrangements that exist within the credit-card system) to merchants, and to a lesser extent to card-issuers and transaction-processing organisations.

It is also necessary, however, to consider the perspective of the various service providers. The perception of unacceptable risk would be likely to result in non-adoption or slow adoption or abandonment (whether by consumers or by merchants), and hence low return on investment and even (as has occurred several times before) outright loss of the investment.

The Threat and Vulnerability Aspects

A threat is a circumstance that could result in harm, and may be natural, accidental or intentional. A vulnerability is a feature or weakness that gives rise to susceptibility to a threat. It is convenient to address both together in a single section.

Second-party threats arise from behaviour, or more particularly misbehaviour, by (from the payer's perspective) the payee. Categories include non-performance (such as failure to deliver or perform in accordance with the contract), and malperformance (such as late delivery or performance, the extraction of funds from the payer's account greater than that authorised or more often than was authorised, and slow and/or unsatisfactory response or outright non-response to enquiries and complaints).

Third party threats arise from organisations and individuals other than the payee, whose behaviour or misbehaviour accidentally or intentionally results in harm. Parties who intentionally cause harm, i.e. attackers, are usefully categorised into the following groups:

- **insiders**, i.e. persons who have authorisation to be on premises, use resources (physically or electronically) and/or access data, but do so for a purpose different from that for which they are authorised;
- **intruders**, who have no authorisation, but contrive to be on premises, use resources (physically or electronically) and/or access data; and
- **once-removed parties**, who in some way take advantage of actions by one or more insiders and/or intruders.

Checklists of threats and vulnerabilities relevant to mobile payments are provided in the following Appendices to this paper:

- the access device itself (Appendix C1);
- use of the access device to conduct transactions (Appendix C2);
- other interactions that take place between the access device and other facilities (Appendix C3);
- the infrastructure that supports mobile transactions (Appendix C4).

A great deal of research has been conducted by computer scientists into the interplay between access devices and the infrastructure that enables eCommerce and M-Commerce. On the other hand, far less consideration has been given to threats that arise from the physical contexts in which access devices are used.

Specific threats include the observation of authenticators, unnoticed and unauthorised use of the device, and possibly of authenticated sessions and processes that are running on it at the time. Categories of perpetrator include fellow householders, friends in social environments, and colleagues in work-environments – and perhaps cleaners, security staff, repairmen and supervisors if the device is left unattended and in a usable state. If the device's capabilities are abused, the authorised user may or may not be aware of it. Furthermore, there may or may not be a way in which the user, or someone acting on the user's behalf, may be able to discover that someone else has used it, and, if so, what for.

The Safeguards Aspect

Several categories of safeguard strategy need to be distinguished. Proactive strategies include avoidance and prevention, and deterrence. Less substantial but nonetheless of value are reactive strategies such as detection, recovery and insurance. Least effective are non-reactive strategies, i.e. self-insurance, 'taking the risk', or putting up with the harm done. An alternative structure for proactive and reactive strategies distinguishes 'before the fact', 'during the fact' and 'after the fact' approaches. Further conventional distinctions are between physical and logical protections; and among technological, organisational and legal measures.

Practical physical measures are not easy to contrive. Mobile devices are small, and in many cases 'always on', including to some extent at least even when the user thinks they have turned them off. Hardware-based protections such as locks and 'dongles' (tokens that must be inserted into ports on the device, in the absence of which the device is disabled) are expensive, inconvenient and impracticable for consumers juggling handhelds. All are subject to countermeasures by attackers. As a result, few consumer devices are subject to them.

Logical safeguards include:

- the prevention of any use being made of the device unless the user demonstrates that they know a specific 'secret', such as a password, PIN, passphrase or choices among icons displayed on the screen. The process of providing such a secret is commonly referred to as 'logging in', and the generic term used is 'identity authentication'. (The term is misleading, however. 'Authority authentication' would be a more reasonable description);
- prevention of the performance of a transaction, even on a logged-in device, until knowledge of a specific 'secret' is demonstrated. This protects against transactions being conducted by a another party who gains possession of a device, if only temporarily, that has been left in a usable state by its authorised user;
- the auto-locking of the device after a period of inactivity, typically 10-15 minutes, forcing authentication to be performed again in order to unlock the device;
- stronger forms of authentication. These typically focus on authentication of the entity rather than the user's identity or the user's authority to transact (Clarke 2003). Biometric applications are available, whereby the device demands periodically that the authorised user's thumb be placed on a reader built into or connected to the device, with the device rendered inoperable if the print does not match sufficiently closely to a pre-recorded reference measure.

Such measures vary greatly in their effectiveness. Many significantly reduce the scope for use of the device by unintended people, but they do not reliably prevent it, because all such logical security safeguards are subject to countermeasures. For example:

- a password may be discovered by watching someone key it in, or by guessing that it is the same as the name of the person, their partner or their pet, or by finding it written down somewhere;
- auto-locking can be avoided by ensuring that the device is used sufficiently frequently that a time-out never occurs;
- a copy of the authorised user's thumbprint can be acquired, and an 'artefact' (such as a latex overlay) can be devised that enables an imposter to masquerade as the authorised user.

Generally, mobile access devices are subject to little in the way of logical security measures. Most users of handhelds are only vaguely aware of the threats, and do not appreciate the harm that could arise if colleagues or visitors use their devices. Few are aware of the available safeguards. Of those who are, many regard the benefits as being too uncertain to justify the inconvenience.

A variety of technological measures have been invented, such as message encryption, digital certificates and the authentication of transaction devices. A few have been deployed, and a very few are even used, but most are ineffective in practice (Clarke 2001b).

Some sets of authentication guidelines propose organisational safeguards based on risk assessment, such as dual-authority for transactions, the application of heuristics to detect risk-prone transactions, the maintenance of log-files, and the audit of log-files for patterns associated with inappropriate transactions. These may be applied where the payer is acting on behalf of a corporation or government agency, or even where they are doing personal business but using an access device or infrastructure provided by their employer. Individuals acting on their own behalf commonly do not have the benefit of such safeguards.

Legal safeguards may exist. In most jurisdictions, however, the expectations of consumers are very poorly supported by consumer protection laws (Clarke 2006). The terms of consumers' relationships with merchants and financial services providers are generally imposed by the corporation rather than negotiated, and serve its own needs far better than those of consumers. Moreover, very few jurisdictions have adapted their consumer protection laws to reflect the realities of mobile payment addressed in this paper. Indeed, financial institutions in at least some countries have been arguing for consumer protection to be reduced, including New Zealand (at this stage successfully) and Australia (so far unsuccessfully. See Clarke & Maurushat 2007).

Implications

In order to provide an initial test of the applicability of the framework, a sample threat / vulnerability / safeguard analysis was undertaken, and consideration given to the implications of the evaluation. This is reported on in Appendix D to this paper. The framework presented in this paper, together with its pilot application, give rise to a variety of implications.

Organisations can assess the security of existing and proposed mobile payment schemes, clarify weaknesses, and identify alternative safeguards. Designers of new schemes, and designers of relevant technologies can use the checklists as guidance, and as motivators for new features.

Consumers could be informed by the paper, although it would be unrealistic to expect many to find it, let alone to commit the effort necessary to grasp its contents and implications. Consumers have little understanding of the risks involved, and little or no control over them. Their rational position would be at least wariness about M-Payment schemes, but perhaps suspicion of them and their sponsors, and even hostility to them.

The framework therefore also has implications for public policy. Payers, especially consumers and micro and small business enterprises, have very little power in comparison with merchant-payees, financial services providers, network services providers, and manufacturers and suppliers of mobile access devices. It is the responsibility of Parliaments to provide a legal context that ensures that mobile payment schemes are subject to appropriate levels of security, and that

appropriately allocates risks. There are ample examples of both market failure and Parliamentary failure. Parliaments may wish to delegate the details of regulatory measures, but they will continue to fail the public need if they bring no pressure to bear to force regulatory agencies and industry associations to impose requirements on scheme designers and operators.

Areas in which regulatory action may be needed include:

- design features;
- audit and certification of designs;
- awareness and education among users of mobile payment schemes;
- the assignment of liabilities;
- the operation of complaints schemes;
- dispute resolution mechanisms; and
- recourse against recalcitrant services providers.

For academics, the framework gives rise to a range of questions that are in need of research. Do consumers have different risk-aversion profiles in a mobile context compared with Internet Commerce and with conventional commerce? To what extent, and under what circumstances, are mobile consumers prepared to trade off convenience against payment risk? To what extent are various consumer segments capable of understanding risk/convenience trade-offs? What reference-points will various consumer segments use in deciding whether to adopt particular payment schemes, and to continue using them? How fragile will trust by consumers be in mobile payment systems? Will a security-related scare reduce adoption, or even halt it, or even reverse the patterns of usage a scheme has achieved? Will a scheme, and will a technology, be able to recover from a justified (or even merely perceived) security-related scare?

It would appear likely that the risk/convenience trade-off will vary, even within a homogeneous consumer segment, and even for the individual consumer, depending on various factors. Is the familiarity of the payment process sufficient assurance to stimulate adoption? How important an adoption factor is the value of the transaction? Does the existence of a prior relationship with the payee make a difference to adoption behaviour?

Conclusions

Mobile payments mechanisms inherit many of the characteristics of the payment schemes that are already in place. These vary greatly in their security profiles, and in their fit to the many different contexts in which payment transactions are conducted.

Conventional credit-card payment is inherently insecure – particularly when conducted under MOTO conditions, particularly over networks, and particularly using mobile access devices. In many cases, debit-card payments may also prove to be much more susceptible to fraud than has been the case with EFTPOS and Internet Banking, because of the context in which data is captured, and the reduced capacity of handheld devices to implement the protections that have been important to the successful deployment of Internet Banking applications.

Mobile payment processes can be quick, intuitive and convenient, and hence need not be an obstacle to M-Commerce. On the other hand, they can be just as quick, intuitive and convenient for an unauthorised user of the access device as for its owner. Financial losses by consumers, and even the perception that they are likely, would appear to be a strong impediment to adoption.

The risk assessment framework presented in this paper provides a means whereby that impediment can be addressed.

References

Unless otherwise noted, all links were accessed during January 2008.

AS/NZS 3931 (1998) `Risk Analysis of Technological Systems - Application Guide' Standards Australia, 1998

AS/NZS 4360 (1999) `Risk Management' Standards Australia, 1995, 1999

Atos (2005) 'Telecoms Predictions 2006', Atos Consulting, at http://www.atosorigin.com/NR/rdonlyres/3AEB9CEF-FB75-4259-9D72-92C66331C7D9/0/rp_Atos_Origin_Predictions.pdf+M-Commerce+growth+predictions+2006&hl=en&ct=clnk&cd=9&client=safari

BIS (2003) 'A glossary of terms used in payments and settlement systems', Committee on Payment and Settlement Systems, Bank for International Settlements, at http://www.bis.org/publ/cpss00b.pdf

BIS (2007) 'Central bank payment system information' Bank for International Settlements, 2007, at http://www.bis.org/cpss/paysysinfo.htm

Chau P.Y.K. & Poon S. (2003) 'Octopus: an e-cash payment system success story' Communications of the ACM 46, 9 (September 2003)

Choi Y.B., Crowgey R.L., Price J.M. & VanPelt J.S. (2006) 'The state-of-the-art of mobile payment architecture and emerging issues'Int. J. of Electronic Finance 1, 1 (2006) 94 - 103

Clarke R. (1990) 'Consumer EFTS in Australia: Security Issues' Comp. & Security Law Reporter 5,5 (January/February 1990)

Clarke R. (1992) 'Case Study Cardomat/Migros: An Open EFT/POS System' Austral. Comp. J. 24,1 (February 1992), at http://www.anu.edu.au/people/Roger.Clarke/EC/Migros.html

Clarke R. (1996a) 'Message Transmission Security (or 'Cryptography in Plain Text')' Privacy Law & Policy Reporter 3, 2 (May 1996), pp. 24-27, at http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html

Clarke R. (1996b) 'The SET Approach to Net-Based Payments' Xamax Consultancy Pty Ltd, November 1996, at http://www.anu.edu.au/people/Roger.Clarke/EC/SETOview.html

Clarke R. (1997) 'Cookies' Xamax Consultancy Pty Ltd, 1997, at http://www.anu.edu.au/people/Roger.Clarke/II/Cookies.html

Clarke R. (1998) 'Europay Switzerland's SVC Project' Xamax Consultancy Pty Ltd, 1998, at http://www.anu.edu.au/people/Roger.Clarke/EC/SVCSwitz.html

Clarke R. (2001a) 'Introduction to Information Security' Xamax Consultancy Pty Ltd, February 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html

Clarke R. (2001b) 'The Fundamental Inadequacies of Conventional Public Key Infrastructure' Proc. Conf. ECIS'2001, Bled, Slovenia, 27-29 June 2001, at http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html

Clarke R. (2003) 'Authentication Re-visited: How Public Key Infrastructure Could Yet Prosper' Proc. 16th Int'l eCommerce Conference, Bled, Slovenia, 9-11 June 2003, at http://www.anu.edu.au/people/Roger.Clarke/EC/Bled03.html

Clarke R. (2006) 'A Major Impediment to B2C Success is ... the Concept 'B2C' Invited Keynote, Proc. ICEC'06, Fredericton NB, Canada, 14-16 August 2006, at http://www.anu.edu.au/people/Roger.Clarke/EC/ICEC06.html

Clarke R. & Maurushat A. (2007) 'The Feasibility of Consumer Device Security' Xamax Consultancy Pty Ltd, April 2007, at http://www.anu.edu.au/people/Roger.Clarke/II/ConsDevSecy.html

Clarke R. & Walters M. (1989) 'Consumer EFTS in Australia: An Introduction' Comp. & Security Law Reporter 5,4, (November/December 1989)

Dahlberg T., Mallata N., Ondrusb J. & Zmijewska A. (2007) 'Past, present and future of mobile payments research: A literature review' Working Paper, February 2007

Davies G. (2002) 'A History of money from ancient times to the present day' University of Wales Press, 3rd. ed., 2002, at http://www.projects.ex.ac.uk/RDavies/arian/llyfr.html

ePayNews.com (2002) 'ePayNews.com Statistics' 2002, at http://www.epaynews.com/statistics/mcommstats.html#47

Grand J. (2004) 'Introduction to Mobile Device Security' Proc. Black Hat Europe 2004 Briefings, Grand Idea Studio, Inc., May 2004, at https://www.blackhat.com/presentations/bh-europe-04/bh-eu-04-grand-mobil.pdf

Gutmann P. (2005?) 'The Convergence of Internet Security Threats (Spam, Viruses, Trojans, Phishing)', at http://www.cs.auckland.ac.nz/~pgut001/pubs/blended.pdf

Herzberg A. (2003) 'Payments and Banking with Mobile Personal Devices' Commun. ACM 46, 5 (May 2003)

ISO (2005) 'Information Technology – Code of practice for information security management', International Standards Organisation, ISO/IEC 27002:2005

Jakobsson M. & Myers S. (eds.) (2006) 'Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft' Wiley, 2006

Kreyer N., Pousttchi K. & Turowski K. (2003) 'Mobile Payment Procedures: Scope and Characteristics' e-Service Journal 2, 3 (Summer 2003) 7-22

Landoll D.J. (2005) 'The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments' CRC, 2005

Lee C., Kou W. & Hu W.C. (Eds.) (2004) 'Advances in Security and Payment Methods for Mobile Commerce' IGI Global, 2004

Leyden J. (2008) 'Bank turns London man into RFID-enabled guinea pig: Halifax customer bites back' The Register, 27 January 2008, at http://www.theregister.co.uk/2008/01/27/paywave/

Linck K., Pousttchi K. & Wiedemann D. G. (2006) 'Security issues in mobile payment from the customer viewpoint' Proc. 14th Euro. Conf. on Information Systems (ECIS), 2006

Misra S.K. & Wickramasinghe N. (2004) 'Security of a mobile transaction: A trust model' Electronic Commerce Research 4, 4 (October 2004) 359–372

Mitnick K.D. & Simon W.L. (2002) 'The Art of Deception: Controlling the Human Element of Security' Wiley, 2002

Moses A. (2008) 'Mobile banking steps up a gear' The Melbourne Age, 31 January 2008, at http://www.theage.com.au/articles/2008/01/31/1201714114004.html

MPF (2006) 'Mobile Proximity Payment Issues and Recommendations: Mobile Payment Configuration and Maintenance' Mobile Payment Forum, v.1.0, October 2006, at http://www.mobilepaymentforum.org/documents/Proximity_Payment_IR_11_0.pdf

OECD (2002) 'OECD Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security' Organisation For Economic Co-Operation And Development, July 2002, at http://www.oecd.org/dataoecd/16/22/15582260.pdf

Paynter J. & Law P. (2001) 'An arm's length evaluation of Octopus' Proc. 1st Int'l Conf. on eCommerce, 2001, at http://www.code.auckland.ac.nz/follow/e-comWorkshop/work%5CAn%20arms%20length%20evaluation%20of%20Octopus.pdf

Peltier T.R. (2005) 'Information Security Risk Analysis, Auerbach, 2nd Edition, 2005

Pousttchi K. (2003) 'Conditions for Acceptance and Usage of Mobile Payment Procedures' In Giaglis G.M., Werthner H., Tschammer V. & Foeschl K. (Eds.) 'mBusiness 2003 - The Second International Conference on Mobile Business' Vienna, 2003 (pp. 201-210), at http://www.wi-mobile.org/fileadmin/Papers/MP/Conditions-for-acceptance-and-usage-of-mobile-payment-procedures_10-07.pdf

Rawson S. (2002) 'E-commerce mobile transactions: Mobility and liability: The hazards of handhelds' Computer Law & Security Report 18, 3 (2002) 164–172

RBA (2007) 'Payments In Other Countries' Reserve Bank of Australia, May 2007, at http://www.rba.gov.au/PaymentsSystem/Publications/PaymentsInOtherCountries/index.html

Recklies O. (2001) 'M-Commerce – the next Hype?' TheManager.org, March 2001, at http://www.themanager.org/pdf/M-Commerce.PDF

Schultz E.E. (2007) 'Mobile computing: The next Pandora's Box' Computers & Security 26, 3 (May 2007) 187, Editorial

Scornavacca E. (2007) 'M-Lit Search' Victoria University of Wellington, at http://www.m-lit.org/

Scornavacca E.,Barnes S.J. & Huff S.L. (2005) 'Mobile Business Research, 2000-2004: Emergence, Current Status, And Future Opportunities' Proc. Euro. Conf. on Information Systems, 2005

Slay J. & Koronios A. (2006) 'Information Technology Security & Risk Management' Wiley, 2006

Stafford T.F. & Andrew Urbaczewski A. (2004) 'Spyware: The Ghost in the Machine' Commun. Association for Information Systems 14 (2004) 291-306, at http://web.njit.edu/~bieber/CIS677F04/stafford-spyware-cais2004.pdf

van der Heijden H. (2002) 'Factors Affecting the Successful Introduction of Mobile Payment Systems' Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 17 - 19, 2002

Visa (2008) 'Visa Authenticated Payment Program', February 2008, at https://partnernetwork.visa.com:443/vpn/global/category.do?userRegion=1&categoryId=85&documentId=117

Vrechopoulos A.P., Constantiou, I.D., Mylonopoulos N. & Sideris I. (2002) 'Critical Success Factors for Accelerating Mobile Commerce Diffusion in Europe' Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 17 - 19, 2002

Wikipedia (2007) 'Computer Insecurity' at http://en.wikipedia.org/wiki/Computer_insecurity, accessed January 2007, plus many articles linked to from the article

Wikipedia (2008' 'Octopus card', at http://en.wikipedia.org/wiki/Octopus_card, accessed January 2008

Zheng X. & Chen D. (2003) 'Study of mobile payments system' Proc. IEEE International Conference on E-Commerce, 2003, 24-27 June 2003, pp. 24- 27

Zmijewska A. (2005) 'Evaluating Wireless Technologies in Mobile Payments – A Customer Centric Approach' Proc. International Conference on Mobile Business (ICMB'05), 2005, pp. 354-362

Appendices

A. A Catalogue of Payment Mechanisms – See Exhibit 1 at http://www.anu.edu.au/people/Roger.Clarke/EC/MP-RAF.html#PMC

B. The Mainstream Security Model – See http://www.anu.edu.au/people/Roger.Clarke/EC/MP-RAF.html#FSM

C. Threats and Vulnerabilities Associated with ...:

1. ... the Access Device – See http://www.anu.edu.au/people/Roger.Clarke/EC/MP-RAF.html#App1
2. ... Transactions – See http://www.anu.edu.au/people/Roger.Clarke/EC/MP-RAF.html#App2
3. ... Other Interactions – See http://www.anu.edu.au/people/Roger.Clarke/EC/MP-RAF.html#App3
4. ... Mobile Infrastructure – See http://www.anu.edu.au/people/Roger.Clarke/EC/MP-RAF.html#App4

D. Application of the Framework – See section 4 of http://www.anu.edu.au/people/Roger.Clarke/EC/MP-RAF.html#FA