Micropayments in Wireless M-Commerce: Issues, Security, and Trend

Journal of Internet Banking and Commerce, July 2004, vol. 9, no.2
(http://www.arraydev.com/commerce/jibc/)

By Xin Luo, Ph.D. Student, Department of Management & Information Systems
College of Business & Industry, Mississippi State University, USA

Web: http://misweb.cbi.msstate.edu/~COBI/faculty/professor.shtml?rluo
Email: xl96@msstate.edu

Xin Luo is currently a doctoral student majoring in Information Systems at Mississippi State University, USA. He has a undergraduate degree in International Business and a Masters degree in Business Administration with a concentration in Computer Information Systems. His research interests center around Information Security, M-commerce, and Wireless communications technology. He is a member of The Mississippi State University Center for Computer Security Research (CCSR).

By Cheon-Pyo Lee, Ph.D. Student, Department of Management & Information Systems
College of Business & Industry, Mississippi State University, USA

Web: http://misweb.cbi.msstate.edu/~COBI/faculty/professor.shtml?cl183
Email: cl183@cobilan.msstate.edu

Cheon-Pyo Lee is currently a doctoral student majoring in Information Systems at Mississippi State University, USA. He has a undergraduate degree in Law, a Masters degree in Business Administration, and a Masters degree in Computer Information Systems. His research interests include E-commerce strategy, Wireless technology, and M-commerce.

Abstract

Although Micropayments were once considered one of the Internet's great failures, the wireless mobile commerce now presents an arena ripe with possibilities to resurrect micropayment technology. Merging these technologies requires serious consideration, including a number of significant security concerns in Bluetooth wireless technology. While a variety of micropayment issues remain unresolved, the future trend of wireless micropayments seems hopeful.

Keywords: micropayments, Internet banking, mobile commerce, security, wireless

Introduction

"You can't use your credit card as a mobile phone, but soon you'll be able to use your phone as a credit card"

Although Nokia's advertisement seems ludicrous today, mobile micropayment technology is slowly making its mark on the mobile commerce (m-commerce) arena. M-commerce is rapidly expanding and is expected to be the second largest industry in the world by 2010 (Rao 2000). Mobile payment systems are an essential part of m-commerce and mobile business (m-business) and will not only make purchasing activities more flexible and convenient but also create unimagined new markets.

Micropayments are any payment under $10 to buy and sell digital goods over the World Wide Web. This payment system offers the ability to handle transactions as small as 1¢. Simply put, micropayments represent the transfer of value from one entity to another in small amounts, where transfer revenue is greater than transfer cost (Jones 2001). Flat-rate subscriptions, pay-per-click, and loyalty points are examples of micropayment applications on the Internet today.

Micropayments received enormous attention back in the '90s and were considered the key to the growing e-commerce market (i.e. Lesk 2004; Solomon 2000). They were also expected to solve thorny financial problems all at once (Shirky 2000). However, micropayments were unable to deliver and have since been considered one of the Internet's great failures (Patch et al. 1998). Financial institutions, consumers, and merchants were reluctant to use micropayments and remained far beyond the scope of the Internet development.

To establish a successful micropayment system, network systems must evolve fully incorporating mobility, accessibility, flexibility and consumer desires. Wireless communications technology provides the essential elements missing in previous micropayments schemes: mobility and accessibility. Today, with the proliferation of wireless networks, mobile devices, and consumers' increasing desire for more purchasing power and convenience, micropayments 'rise out of the trash can' (Lesk 2004; Wilson 2000). The year 2003 witnessed a significant expansion in the number of schemes using mobile devices to facilitate payment such as for electronic newspapers, subway tickets, and car parking fees. These pilot programs were particularly successful in Western Europe and Asia.

Issues

A New Framework and New Era for Financial Institutions

As the mobile payment market rapidly increases, a new relationship between wireless providers and banks needs to be established. Traditionally, according to the secure electronic transaction (SET) model, payment services are supplied primarily by the banking system and typically are regulated by the central bank as an important adjunct to implementing monetary policy (Hancock et al. 1998). However, in the mobile payment market, wireless carriers employing their customer base, technical know-how, and billing experience will play an active role in the mobile payment market as mobile users access their networks to perform all transactions (Varshney 2003), and as the role of wireless carriers increases, the tensions between wireless carriers and banks (Hoffman 2001) as well as new strategic alliances are frequently observed. Finnish telecommunications operator Sonera Corp., conducts a pilot of its own mobile payment service without the involvement of banks (Hoffman 2001), and SK Telecom, a South Korea wireless service provider, has launched a m-payment service called NEMO ("Net money", http://www.nemo.co.kr) through a strategic alliance with several banks. In any case, banks must prepare for a new era with mobile network operators and innovative financial institutions that recognize that the key to success in micropayments is volume of transactions, and that work together to create the scale of trading community required. In the new era, a cooperation must be established for banks and operators to smoothly make mobile billing systems work in terms of instant credit card/checking account charge, E-Money, and stored value accounts. Further, Costello (2003) indicates that stored value account operators must ensure that they are protected from charge-backs on fund load operations, and can benefit through partnerships that offer funds loading through ATMs and on-line banking interfaces.

Creating Markets for Mobile Payment

"People do not buy content the same way they do candy" (Smith 2003). This is the best lesson which wireless micropayments should learn from the struggling of wired micropayments. According to Kearney's m-commerce survey (Kearney 2004), more customers tend to use micropayment systems,

especially for small cash transactions such as transit fare or vending machines. Mobile micropayments have already reached markets in regions such as South Korea, Japan, and Hong Kong as well as Western Europe. Smart coke machines can transmit data back to company warehouses calling for coke restock (Mendez-Wilson 2000); NEMO (Net-Money) of SK Telecom enables users to pay transit fare using their handsets. Micropayments vendors predict that new types of content will fuel future demand for their products (Essex 1999). Well-established small transaction markets for mobile transactions, in addition to various service providers and content providers, are believed to be essential components to reach high actual usage rate for mobile payment (Lee et al. 2004).

Establishing a Critical Mass of Sellers and Buyers

One of important features of e-commerce technologies such as electronic payment system is that multiple groups must jointly adopt the system in order for it to succeed (Plouffe et al. 2001). Customer survey data also consistently show that widespread acceptance of the system by its participants is a very important factor in payment adoption (Panurach 1996). In other words, customers would use the system because most sellers use it. Therefore, the growth of mobile payment market is not possible without high participation of merchants.

In the wired micropayments market, too much extra work for merchants, such as installing special software or creating links to vendor Web site, prevents merchants from adopting the payment system (Solomon 2000). Therefore, simple and easier installing processes are needed to attract more merchants to implement the mobile micropayment system. Also, for merchants, one benefit of using the micropayment vendor which has a strong brand and large member base would be attracting more customers to the store. Like familiar credit card brands which offer a feeling of trust for customers (Karpinski 1999), mobile payment merchants need the vendors which will generate traffic for merchants through their brands.

Security

Bluetooth wireless technology has appeared on many mobile devices such as mobile phones and PDAs. It is a specification for short-range, low-cost, and small form-factor that enables user-friendly connectivity among portable and handheld personal devices, and provides connectivity of these devices to the Internet (Bisdikian 2001). Thus, Bluetooth-powered mobile devices seem a perfect tool for micropayments over the networks, because Bluetooth technology can easily offer accessibility and mobility to mobile users.

However, while providing immense benefit, the use of Bluetooth-enabled mobile phones for micropayment triggers new risks. Our wireless networks are not as resistant as the wired ones. Information can be intercepted in the open airwave. Recent reports of successful hacks into some Bluetooth-enabled cell phones have raised security concerns. Yet mobile phone vendors are facing a dilemma between security against ease-of-use concerns. Those focused on consumers are more concerned about ease of use and may not take full advantage of the Bluetooth specification's security options, such as its encryption and authentication features (Mitchell 2004). Nevertheless, in addition to function, mobile customers are also concerned about security issues in the unprotected air, such as sending confidential data, making purchase, or paying bills via mobile technology networks. Sahut et al. (2004) indicate that credit card security concerns prevent 52 % of customers from adopting m-commerce via phone and 47 % via PDA, according to a Forrester Research survey (Sahut et al. 2004).

Thus, mobile customers must be careful when they turn on their Bluetooth-enabled phones, because they could unknowingly open the door to an intruder who could steal confidential information such as address book or even use phone to make expensive calls (Blau 2004), triggering a potential threat to micropayments. Several serious vulnerabilities in some Bluetooth-enabled phones have been discovered:

- The SNARF attack: confidential data can be obtained, anonymously, and without the owner's knowledge or consent, from some Bluetooth enabled mobile phones. (Brewin 2004) The data include, at least, the entire phonebook and calendar, and the phone's IMEI (International Mobile Equipment Identity), which uniquely identifies the phone to the mobile network, and is used in illegal phone 'cloning').

- The BACKDOOR attack: involves establishing a trust relationship through the "pairing" mechanism. In this way, the attacker may be free to use any resource that a trusted relationship with that device grants access to. This means that not only can data be retrieved from the phone, but other services, such as modems or Internet, WAP and GPRS gateways may be accessed without the owner's knowledge or consent (Laurie et al. 2004).

- The BLUEBUG attack: creates a serial profile connection to the device, thereby giving full access to the AT command set. With this facility, it is possible to use the phone to initiate calls to premium rate numbers, send SMS messages, read SMS messages, connect to data services such as the Internet, and even monitor conversations in the vicinity of the phone. Call forwarding diverts can be set up, allowing the owner's incoming calls to be intercepted (Laurie et al. 2004).

- Bluejacking: involves sending unsolicited text messages to other Bluetooth users. (Brewin 2004) If such an event occurs, then all data on the target device becomes available to the initiator, including such things as phone books, calendars, pictures and text messages as well as important micropayment information including account number or credit card number (Laurie et al. 2004).

Notwithstanding the current security concerns listed above, Bluetooth is considered more secure than any other wireless technology, such as Wi-Fi which is vulnerable to security threats due to its weak WEP and WPA protocols and the predicament that 802.11i standard is yet to be ratified. Bluetooth wireless technology still prevails in the mobile communications market because of the short transmission range of most devices and its 128-bit encryption capabilities. It will be one of the major technical forces pushing the popularity of wireless micropayments in the m-commerce arena. Even with the security concerns existing in some Bluetooth-enabled mobile phones, serious wireless micropayments security problems, such as loss of stored value account number or E-money, have not yet surfaced. And it is expected that the next generations of mobile wireless phone system (3G & 4G) would not encounter any serious security threats as the mobile phone vendors are proactively dealing with the existing as well as potential security threats. Meanwhile, wireless micropayment participants, such as mobile service providers and financial institutions, will need to better educate mobile customers to arouse their awareness of the potential threats existing in the air. Finally, we expect that relevant wireless micropayments information policies, the foundation of information security within the new framework, will be established to further underpin security and well being of information resources in the open airwave.

Conclusion and Future of Wireless Micropayment

There are many reasons behind micropayments' slow growth over the Internet, such as the increasing flexibility of the existing financial framework (i.e., credit card) (Odlyzko 2003), complicate pricing (Shirky 2000), and unpredictable transaction. Also, the popularity of conventional payment devices, particularly in the Unites States, explains why innovative payment systems are not yet successful in this market (Dekleva 2000). However, the biggest reason of micropayments' struggling over the internet was user disapproval. In other words, micropayments systems failed because the systems didn't know what users and merchants actually need. Getting user's approval with reliable and secure networks will be a big challenge to wireless micropayments.

Looking ahead, the continued push towards the integration of RFID chips with mobile phones will begin to generate significant transaction volumes over the next few years. It is predicted that the continued growth of wireless technology in European markets will drive significant growth in mobile payments in Europe from 2005 onwards. From a global perspective, m-payment generated sales are estimated to reach $25 billion in 2008 (Taylor 2004).

While it is not clear whether the new attempts to implement micropayments systems will be successful, the ultimate success of wireless micropayments systems will depend on a number of critical issues, such as a new framework and new era for financial institutions and operators, creating markets for mobile payment, establishing a critical mass of sellers and buyers, and wireless communications information assurance. The rapid development of state-of-the-art technologies such as Bluetooth and Wi-Fi continues to entice more businesses (i.e. banks, credit card companies, and service/good vendors) to participate, providing a hotbed for micropayments transactions and stimulating mobile

customers to embrace wireless micropayments, which, in turn, will eventually broaden the market.

Acknowledgement

A number of people have generously given valuable time and effort towards this article. The authors appreciate Dr. Merrill Warkentin and Dr. J.P. Shim, Professors of Management Information Systems of Mississippi State University, for their research directions and suggestions. Also, the authors thank Dr. Ray Vaughn for the support of CCSR.

References

Abrzahevich, D. "Electronic Payment Systems: Issues of User Acceptance," Accessed February 18, 2004 (available online at http://www.ipo.tue.nl/homepages/dabrazhe/ps/Library/data/ebiz2001.PDF)

Bisdikian, C. "An overview of the Bluetooth wireless technology," *IEEE Communications Magazine* (39:12), December 2001, pp 86-94.

Blau, J. "Cracks appear in Bluetooth security," *Computerworld*, February 11 2004.

Brewin, B. "Security threats raise concerns about Bluetooth," *Computerworld*, May 10 2004.

Costello, D. "Micropayment and Mobility," online: http://www.epaynews.com/downloads/zafion_WP.pdf, June 2003.

Dekleva, S. "E-Commerce: A Half Empty Glass?" *Communications of the Association for Information Systems* (3:18) 2000.

Dekleva, S. "M-Business: Economy Driver or a Mess?" *Communications of the Association for Information Systems* (13:11) 2004, pp 111-135.

Essex, D. "Big dreams for tiny money," *Computerworld* (33:50) 1999, p 66.

Hancock, D., and Humphrey, D. "Payment transactions, instruments, and systems: A survey," *Journal of Banking & Finance* (21) 1998, pp 1573-1624.

Herzberg, A. "Safeguarding Digital Library Contents: Charging for Online Content," *D-Lib Magazine*, January 1998.

Hoffman, K.E. "New options in wireless payments," *Internet World* (7:7) 2001, p 37.

Jones, R. "Micropayment Architectures," The NuVantage Group, online: http://www.webguild.org/presentations/micropayment.pdf) 2001.

Karpinski, R. "Round two for internet payments," *Internetweek.com* 1999.

Kearney, A.T. "Mobinet 5," Accessed February 18, 2004 (available online at http://www.atkearney.com/main.taf?p=5,4,1,60)

Laurie, A., and Laurie, B. "Serious flaws in bluetooth security lead to disclosure of personal data," *ADL Press Release* 2004.

Lee, C.P., Warkentin, M., and Choi, H. "The Role of Technological and Social Factors on the Adoption of Mobile Payment Technologies," *Proceeding of Americas Conference on Information Systems*, New York, 2004.

Lesk, M. "Micropayments: An idea whose time has possed twice?" *IEEE Security & Privacy* (2:1), 2004, pp. 61-63.

Mendez-Wilson, D. "Goodbye cash and credit cards" *Wireless Week* (6:44) 2000, pp 32

Mitchell, R.L. "Bluetooth at the Gates" *Computerworld*, May 17 2004.

Odlyzko, A. "The case against micropayments," *7th International conference financial cryptography*, Springer, 2003.

Panurach, P. "Money in electronic commerce: Digital cash, electronic fund transfer, and ecash," *Communications of the ACM* (39:6) 1996, pp 45-50.

Patch, K., and Smalley, E. "Drop a dime online," *InfoWorld* (20:48) 1998, p 71.

Plouffe, C.R., Vandenbosch, M., and Hulland, J. "Intermediating technologies and multi-group adoption: A comparison of consumer and merchant adoption intentions toward a new electronic payment system," *The Journal of Product Innovation Management* (18) 2001, pp 65-81.

Quain, J.R. "Can You Spare Some Change?" *PC Magazine* (22:23) 2003, p 26.

Rao, M. "South Korea Aims for Global Leadership in Wireless, Broadband Internet Markets in Information Age," Accessed February 18, 2004 (available online at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan006689.pdf) (2003: September 1) 2000.

Sahut, J., and Galuszewska, M. "Why does SSL dominate the e-payment market?" *Journal of Internet Banking and Commerce* (9:1) 2004.

Shirky, C. "The case against micropayments," Accessed February 18, 2004 (available online at http://www.openp2p.com/lpt/a/515) (2003:Nov.15) 2000.

Smith, S. "Are micropayments promising or penny-ante?" *EContent* (26:10) 2003, p 23.

Solomon, M. "Micropayments," *Computerworld* (34:18) 2000, p 62.

Taylor, P. "M-Parking Still Leads the M-Payment Pack," *Strategy Analytics Report*, January 2004, p 3.

Varshney, U. "Wireless I: Mobile and wireless information systems: applications, networks, and research problems," *Communications of the Association for Information Systems* (12:11) 2003, pp 1-23.

Wilson, T. "Micropayments rise out of the trash can," Accessed February 18, 2004 (available online at http://www.internetweek.com/columns00/bits030600.htm (2003:Feb. 15) 2000.