MOBILE COMMERCE

Secure Mobile Payment Systems

Jesús Téllez Isaac, *Universidad de Carabobo, Venezuela*
Sherali Zeadally, *University of Kentucky*

Recent technological advances have accelerated the design and worldwide deployment of mobile payment systems, yet security remains a paramount concern. Designers must consider many security issues and possible solutions. They must also keep an eye on future challenges and opportunities.

The worldwide proliferation of the Internet has led to the emergence of an extensive range of services—one of the most popular being electronic commerce (e-commerce).[1] Recent technological advances in the design of portable devices, along with increasing high-speed Internet access and mobile networking technologies, have enabled users to employ such devices anywhere, anytime to perform e-commerce transactions in addition to operations such as browsing the Web and reading email.[2] The wireless technological revolution has enabled mobile devices to become a critical component of the new digital economy, in which users execute transactions while on the move.

Mobile e-commerce (or *m-commerce*) is considered a natural extension of e-commerce and represents a new way for conducting commerce.[3,4] M-commerce refers to e-commerce transactions conducted through a mobile device via wireless networks. The electronic payment performed in wireless environments leads to the term *mobile payment* (or *m-payment*), which is defined as any payment transaction involving the purchase of goods or services that is completed with a wireless device. M-payments facilitate m-commerce because they let users make online purchases from their mobile devices remotely at any time.

We present the major security issues that must be taken into consideration when designing,

1520-9202/14/$31.00 © 2014 IEEE

implementing, and deploying secure m-payment systems. In particular, we focus on threats, vulnerabilities, and risks associated with such systems as well as corresponding protection solutions to mitigate these risks. We also discuss some of the challenges that need to be addressed in the future as m-payment systems become fully integrated with other emerging technologies such as fifth-generation mobile networks (5G) and cloud computing.

Mobile Payment Systems

A mobile payment system (MPS) can be defined as any payment system that enables financial transactions to be made securely from one organization or individual to another over a mobile network (using a mobile device).[5,6] M-payment offers attractive opportunities to financial institutions, merchants, and users. These opportunities include the simplicity and ease of an m-payment transaction for the user; they also enable merchants to access customer information and target specific customer groups through various incentive programs, such as discount coupons and rewards programs.

The number of m-payment users continues to increase exponentially. The growth of m-payment transactions over the last decade has been largely enabled by increasing speeds of mobile-network connections, the rapid proliferation of portable devices (such as mobile-connected tablets), and the worldwide penetration of mobile-cellular subscriptions, which reached 96 percent in 2013 and 40 percent of the world's population using the Internet.[7] In fact, the global worldwide m-payment market will reach over 450 million users and a transaction value of over US$721 billion by 2017, according to a Gartner group forecast.[8]

The main entities of an m-payment system and their interactions during an m-payment transaction are illustrated in Figure 1. Generally, an m-payment system consists of four main entities: the client, the merchant, the merchant's financial institution (called the *acquirer*) and the client's financial institution (called the *issuer*). The client and the merchant can be connected through a short-range link or the Internet using wired, wireless, or cellular communication technologies that are offered by a mobile-phone operator (such as General Packet Radio Service (GPRS), Enhanced Data Rates for Global System for Mobile Communications (GSM) Evolution, Evolution-Data Optimized, or High Speed Downlink Packet Access (HSDPA)).

However, an m-payment system can also comprise a client, a merchant, and a payment gateway, which is an additional entity acting as an intermediate for payment-clearing purposes between the acquirer and the issuer on the bank's private network side and between the client and the merchant on the Internet side.[9] The connection between the client and the payment gateway or between the merchant and the payment gateway can be set up through any Internet access service provided by an Internet service provider or the Internet, using wired, wireless, or cellular communication technologies offered by a mobile-phone operator. The connections among the issuer, the acquirer, and the payment gateway typically occur over the private (wired) networks of banks, and the communication is made secure using well-known security protocols (for example, Secure Socket Layer/Transport Layer Security).

Classifying M-payments

M-payments can be classified in various ways. Currently, one of the universally accepted ways to classify an m-payment is as either

- *a remote payment*, where the user makes a payment using a mobile device to access the m-payment back-end system via mobile communication networks, or
- *a proximity payment*, where the user makes a payment using a mobile device and short-range communication technologies.[8]

This article considers a much broader m-payment classification based on several other criteria, including

- basis of payment, or how the money is transferred;
- payment medium to be used to realize the payment;
- timing of payment, or when it occurs;
- payment amount conveyed from the customer to the merchant; and
- payment location—that is, where the payment takes place.

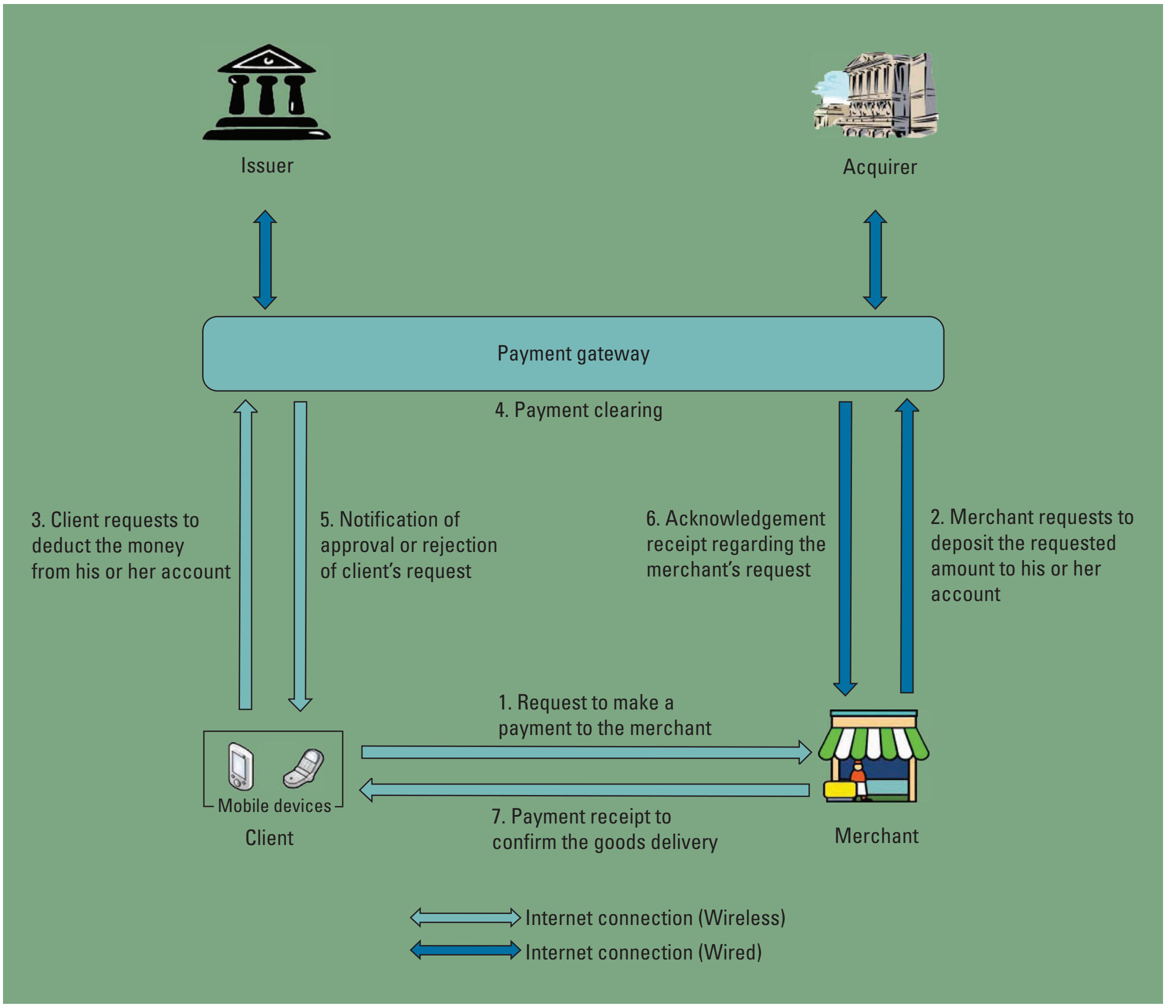
Issuer
Acquirer
Payment gateway
4. Payment clearing
3. Client requests to deduct the money from his or her account
5. Notification of approval or rejection of client's request
6. Acknowledgement receipt regarding the merchant's request
2. Merchant requests to deposit the requested amount to his or her account
1. Request to make a payment to the merchant
Mobile devices
Client
7. Payment receipt to confirm the goods delivery
Merchant
Internet connection (Wireless)
Internet connection (Wired)

Figure 1. Typical entities of a mobile-payment system and their interactions during a mobile-payment transaction.

Table 1 presents the classification of m-payments considering these criteria.[10–13]

Client-Side Technologies for M-payments

The following technologies, some of which are still emerging and maturing, are used to implement m-payments on the client side.

Short message service. This service allows mobile systems and other networked devices to exchange short text messages with a maximum length of 160 characters. SMS is available on a wide range of networks and is popular with both individuals and businesses.

Unstructured supplementary services delivery. This session-based, transaction-oriented technology is unique to GSM and refers to the capability built into the GSM standard for supporting the transmission of information over the GSM network's signaling channels.

Wireless application protocol/GPRS. GPRS is a mobile data service available to GSM users that enables WAP-enabled devices such as mobile phones to support services such as Internet browsing, multimedia messaging service, and Internet-based communication services such as email and World Wide Web access.

Phone-based application. The m-payment client application (residing on the consumer's mobile phone) can be developed using the Java 2 Platform, Micro Edition for GSM-based mobile phones and the Binary Runtime Environment for Wireless for mobile phones based on code division multiple access.

Table 1. Existing m-payment methods.[11–13]

M-payment criteria	Methods
Basis of payment	*Account-based*: Every consumer is associated with a specific account maintained by an Internet payment provider (IPP) and is periodically billed and pays for the balance of the account to the IPP.
	Token-based: An electronic token is a medium of exchange representing a monetary value, usually supported by a bank. Consumers convert actual currency to an electronic equivalent with their issuer before making a transaction. A merchant collects the tokens and sends them to the acquirer to redeem the money.
Payment medium	*Mobile payment by bank account or credit card*: with or without direct access to the card during the payment.
	Mobile payment by phone.
Timing of payment	*Real-time (cash)*: Payment methods adopt a real-time or cash-like payment schedule that involves some form of electronic currency that is exchanged during a transaction.
	Prepaid (debit): Consumers pay in advance to obtain the goods they want.
	Postpaid (credit): Consumers receive the goods and consume them before paying.
Payment amount	*Picopayments*: for transaction amounts less than US$0.10.
	Micropayments: for amounts between $0.11 and $10.
	Macropayments: for amounts exceeding $10.
Payment location	*Remote transactions*: conducted independent of the user's location.
	Proximity or local transactions: The mobile device communicates locally with other devices using short-range communication technologies.

SIM-based application. The Subscriber Identity Module (SIM) used in GSM mobile phones is a smart card whose information can be protected using cryptographic algorithms and keys. (Smart cards are microcomputers small enough to fit in a wallet or even a mobile phone. They have their own processors and memory for storage.) SIM applications are relatively more secure than client applications that reside on the mobile phone.[14]

RFID. This technology uses radio frequency (RF) signals to exchange data between a reader and an electronic tag attached to an object, for the purpose of ID and tracking.

Near-field communication. This short-range wireless communication standard results from the fusion of the contactless smart card (RFID) and the mobile phone.[15]

SIM application toolkit. This technology allows configuration and programming of the SIM card.

Voice-based payment transactions. These can be done by making a phone call to a special number and providing a credit card number.

Dual chip. Dual-chip phones have two slots: one for a SIM card (telephony) and another for a payment chip card. This solution allows an m-payment application provider to develop an m-payment application in the payment chip card without collaborating with the telecommunications operator (the owner of the SIM card).

Mobile wallet. This m-payment application software on the mobile phone contains details of the customer (including bank account details and/or credit card information) that enable the customer to make payments using the mobile phone.

Security Issues for M-Payment Systems

In mobile commerce, security is the biggest issue: without secure commercial information exchange and safe electronic financial transactions over mobile networks, no one will trust m-commerce. M-payment systems transmit sensitive data, so secure communications and transfers are imperative. Thus, for widespread use and customer acceptance of m-payment services, both perceived and technical levels of security must be high.[16,17] Various mobile security procedures and payment methods have been proposed and applied to m-commerce.

Security Vulnerabilities and Solutions

As mentioned earlier, m-payment systems rely on underlying communication technologies (such as

Table 2. Vulnerabilities, threats, risks, and protection solutions in m-payment systems.[18,20]

Vulnerability	Threat	Risk	Protection solutions
Over-the-air (OTA) transmission between a phone and point of sale (POS)	Interception of traffic	Identity theft, information disclosure, replay attacks	Trusted platform module (TPM), secure protocols, encryption
Inadvertent installation by users of malicious software on mobile phones	Downloaded application intercept of authentication data	Theft of authentication parameters, information disclosure, transaction repudiation	Authentication of user (PIN) and application (digital signature by trusted third party), TPM, anti-malware/spyware/virus
Absence of two-factor authentication	User masquerading	Fraudulent transactions, provider liabilities	Two-factor authentication
Changing or replacing a mobile phone	Configuration and setup complexity	Reduced adoption of the technology, "security by obscurity"	Simplified user interface, security parameters in TPM set by a trusted party
Smartphone Internet and geolocation capabilities	Malware on mobile devices, poor data protection controls by merchants or payment processors	Data disclosure and privacy infringement, profiling of user behavior	User control of geolocation features, cryptographically supported privacy, TPM, vetted authorization and accounting
POS devices installed at merchant premises	Masquerade attacks, tampering with POS	Theft of service, replay, message modification	POS vendor vetting, message authenticators, vetted authorization and accounting
Lack of digital rights management (DRM) on the mobile device	Illegal distribution of content (such as, ringtones, video, or games)	Theft of content, digital piracy, risk to provider for digital rights infringement, loss of revenue to content provider or merchant	DRM incorporated in smartphone TPM design, cryptographically supported DRM
Weakness of GSM encryption for OTA transmission, SMS data in cleartext on a mobile network	Message modification, replay of transactions, evasion of fraud controls	Theft of service or content, loss of revenue, illegal transfer of funds	Strong cryptographic protocols, SMS message authenticators, encryption
Weakness of GSM protocol for mutual authentication	Impersonation or man-in-the-middle attacks	Eavesdrop, modify, delete, reorder, replay, and spoof signaling and user data messages	Mutual entity authentication
Weakness of encryption technique on SIM cards	Tampering or cloning of SIM card	Malicious transactions carried out on user's behalf, theft of stored payment credentials	SMS firewall on phone, state-of-art cryptography with sufficiently long keys, PIN for SIM card
Weak cryptographic keys or predictable random-number cryptographic APIs provided by development platforms	Cryptanalysis and dictionary attacks	Unauthorized access to restricted functionalities	Secure third-party cryptography APIs with algorithms that can generate unpredictable random numbers and strong cryptographic keys

GSM, Bluetooth, and RFID) whose security vulnerabilities are often ignored when the security aspects of the m-payment systems are analyzed. Therefore, m-payment system designers should take a holistic view when performing a security analysis during design and implementation.[18] In general, to counter potential threats, a secure m-payment system must satisfy the following transaction security properties: authentication, confidentiality, integrity, authorization, availability, nonrepudiation (ensuring that users can't claim that a transaction occurred without their knowledge), and accountability (defined as the ability to show that the parties who engage in the system are responsible for the transaction related to them[2,19]).

Table 2 summarizes the types of vulnerabilities and threats and their corresponding risks in an m-payment system environment together with relevant protection solutions.[20]

Cryptography

Cryptography techniques play an important role in satisfying the transaction security properties mentioned earlier. They're essential in securing m-payments over open networks that have little or no physical security. *Symmetric cryptography* shares a secret between two parties (a *sender* and a *receiver*) who want to communicate safely without revealing details of the message. Symmetric cryptographic methods are suitable because of their low computational requirements.

However, key management in symmetric-key operations is complex. To solve this complexity, *public-key cryptography* uses a pair of keys for every party: a *public* key (that is published) and a *private* key (that remains secret). Thus, it is not necessary to share a secret key between the sender and the receiver before communicating securely. However, traditional asymmetric signature schemes make the signature computations expensive and aren't suitable for mobile devices. Moreover, to avoid impersonation attacks, for every public key, a certificate is required and must be verified by a certification authority, causing an additional information exchange (and increased delays) during each transaction.[21]

Future Challenges and Opportunities

Mobile communication continues to evolve and improve, and new technologies offering attractive business opportunities are emerging. Solutions provided by m-payment vendors must evolve in order to support increasingly sophisticated client applications running on mobile devices.[16] At the same time, designers must continuously adapt existing m-payment systems to allow clients to take advantage of the benefits associated with emerging technologies while simultaneously ensuring secure and reliable payment transactions. We have identified several challenges and opportunities.

5G Technology

The 5G mobile communications technology is the next generation of the existing 4G Long-Term Evolution network technology. It will enable users to transmit massive data files including high-quality digital movies practically without limitation, allowing subscribers to enjoy a wide range of services, such as 3D movies and games, real-time streaming of ultra-high-definition content, and remote medical services. 5G will enable software-defined radio and flexibility in encryption method used.

Furthermore, 5G will improve latency, battery consumption, cost, and reliability, which will reduce the cost of communications over wireless networks when performing payment transactions. Heterogeneous wireless networking technologies will continue to play a fundamental role in the deployment of 5G networks. However, the disparity of security solutions used by different wireless, mobile, cellular networks makes end-to-end security solutions still a significant challenge that must be addressed to support future secure m-payment systems and applications.

Cloud Computing

A cloud-based m-payment system is a type of proximity payment that stores payment credentials (used to authenticate the payment transaction) on a remote server rather than at the mobile device. To use this solution, both the consumer and the merchant must download the cloud-based application and subscribe to the service. The physical mobile phone might not be needed to complete the payment, depending on the exact solution. Consumers can access their account information in the cloud via mobile devices. In addition, payment notification can be communicated via email or SMS text messages once a cloud payment is completed.[22]

Despite the benefits offered by cloud-based m-payment systems, some security issues remain unsolved. For example, payment data and stored payment credentials in the cloud could be compromised if the cloud server is attacked. Also, payment data should not be transmitted via SMS or email because cloud platforms aren't encrypted. Finally, data privacy remains a key concern for payment data stored in the cloud, which could share this information with other businesses without the consumer's explicit approval.

Security versus Performance

Payment systems that support electronic transactions in wireless networks must have the same levels of security as those designed to support electronic-payment transactions on fixed networks. Moreover, m-payment applications should be compatible with the existing infrastructure of traditional electronic-payment applications so that the existing infrastructure can continue to operate. However, the execution of payment transactions in wireless environments suffers from a number of limitations that require designers of wireless payment systems to find innovative solutions to address these constraints. A possible solution is to reduce the computational requirements of the secure protocols used or to replace the highly computing-intensive cryptographic operations with smarter and more efficient cryptographic protocols requiring less computing and memory resources. As a result, we need a careful tradeoff between transaction performance and its security for secure m-payments.

Restricted Connectivity Scenario

Most of the m-payment systems proposed in the last decade have been based on a scenario where all the entities are directly connected to each other (formally called the *full connectivity scenario*). These m-payment systems do not consider the situation where two entities of the model cannot directly communicate with each other because of a communication restriction (for example, a merchant who can't communicate directly with the payment gateway because of the absence of Internet access on the premises)—a scenario often referred to as *restricted connectivity*. In this context, we define a restricted connectivity scenario as one where two entities of an m-payment system can't communicate with each other directly and must do it through a third party.[23] Despite the new challenges introduced by the restricted connectivity scenario, designers of m-payment systems should provide the same security levels as those based on the full connectivity scenario.

Encryption Technology

Elliptic curve cryptography (ECC) is an alternative approach to public-key cryptography. It relies on the elliptic curve logarithm, which dramatically decreases the key size needed to achieve the same level of security offered in conventional public-key cryptographic schemes. This allows ECC to provide similar security as RSA but using much smaller key sizes (approximately one-eighth of the key size used by RSA), which in turn significantly reduces processing overhead. Therefore, faster computations, lower power consumption and memory, and bandwidth savings are properties offered by ECC that are useful for implementing encryption on resource-constrained mobile devices. In the future, system designers should explore the possibility of incorporating ECC algorithms in existing or new m-payment systems to reap many of the benefits of ECC in mobile devices.

Self-certified public-key schemes (where public-key authentication can be achieved implicitly with signature verification) are an alternative security solution for m-payment systems based on restricted communication scenarios, where an engaging party has connectivity restrictions that prevent communication with a certification authority for validating a certificate during a transaction. In those schemes, the user's public key is derived from the signature of his or her secret key along with his or her identity, and is signed by the system authority using the system's secret key. However, the expiration of this kind of certificate isn't defined in all the schemes proposed in the literature and is an open problem that still must be solved.

M-payment systems will continue to receive a lot of attention by industry and academia. The statistical trends reported in this article indicate that we'll continue to see explosive growth in the number of m-payment users and m-payment transactions. At the same time, security will continue to be a paramount issue. The deployment and adoption of various emerging technologies bring new challenges and opportunities to the design and implementation of secure m-payment systems today and in the future. IT

Acknowledgments

We thank the anonymous reviewers for their valuable comments, which helped us to improve the quality and presentation of this article. We also thank the guest editors for their support throughout the preparation of this article.

References

1. H.-C. Yu, K.-H. Hsi, and P.-J. Kuo, "Electronic Payment Systems: An Analysis and Comparison of Types," *Technology in Society*, vol. 24, no. 3, 2002, pp. 331–347.
2. S. Kungpisdan, "Design and Analysis of Secure Mobile Payment Systems," PhD dissertation, Faculty of Information Technology, Monash Univ., 2005.
3. N. Kshetri and S. Acharya, "Mobile Payments in Emerging Markets," *IT Professional*, vol. 14, no. 4, 2012, pp. 9–13.

4. M. Niranjanamurthy et al., "M-commerce: Security Challenges Issues and Recommended Secure Payment Method," *Int'l J. Management, IT and Engineering*, vol. 2, no. 8, 2012, pp. 374–393.
5. T. Halonen, "A System for Secure Mobile Payment Transactions," master's thesis, Dept. of Computer Science, Helsinki Univ. of Technology, 2002.
6. H. van der Heijden, "Factors Affecting the Successful Introduction of Mobile Payment Systems," *Proc. 15th Bled eCommerce Conf.*, 2002, pp. 430–443.
7. P. Wang et al., "Key ICT Indicators for Developed and Developing Countries and the World (Total and Penetration Rates)," World Telecommunication/ICT Indicators Database, 17th ed., Int'l Telecommunication Union, 2013; www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls.
8. P. Wang et al., "Trends and Prospects of Mobile Payment Industry in China 2012-2015—Creating Innovative Models, Boosting Mobile Financial Services," Financial Services Industry Center of Excellence, Deloitte China, 2012; www.deloitte.com/assets/Dcom-China/Local%20Assets/Documents/Industries/Financial%20services/cn_gfsi_TrendsProspectsChina MobilePaymentIndustry_041212.pdf.
9. J.T. Isaac, S. Zeadally, and J.S. Camara, "Implementation and Performance Evaluation of a Payment Protocol for Vehicular Ad Hoc Networks," *Electronic Commerce Research*, vol. 10, no. 2, 2010, pp. 209–233.
10. B. Singh and K.S. Jasmine, "Comparative Study on Various Methods and Types of Mobile Payment System," *Int'l Conf. Advances in Mobile Network, Communication and Its Applications* (MNCAPPS 12), 2012, pp. 143–148.
11. X. Zheng and D. Chen, "Study of Mobile Payments System," *Proc. IEEE Int'l Conf. E-Commerce* (CEC 03), 2003, pp. 24–27.
12. W. Guo, "Design of Architecture for Mobile Payments System," *Proc. 26th Chinese Control and Decision Conf.* (CCDC 08), 2008, pp. 1732–1735.
13. E. Ramezani, "Mobile Payments," 2008; http://webuser.hs-furtwangen.de/heindl/ebte-08-ss-mobile-payment-Ramezani.pdf.
14. B. Ozdenizci et al., "NFC Loyal: A Beneficial Model to Promote Loyalty on Smart Cards of Mobile Devices," *Proc. Int'l Conf. Internet Technology and Secured Transactions* (ICITST 10), 2010, pp. 1–6.
15. L. Francis et al., "A Security Framework Model with Communication Protocol Translator Interface for Enhancing NFC Transactions," *Proc. 6th Advanced Int'l Conf. Telecommunications* (AICT 10), 2010, pp. 452–461.
16. S. Kadhiwal and M.A.U.S. Zulfiquar, "Analysis of Mobile Payment Security Measures and Different Standards," *Computer Fraud & Security*, vol. 2007, no. 6, 2007, pp. 12–16.
17. V. Lazarov, N. Degefa, and S. Seid, "Secure Mobile Payments," 2008; http://home.in.tum.de/lazarov/html-data/files/research/papers/payments-report.pdf.
18. S. Agarwal et al., "Security Issues in Mobile Payment Systems," *Proc. 5th Int'l Conf. E-Governance*, 2007, pp. 142–152.
19. S. Duangphasuk, M.Warasart, and S. Kungpisdan, "Design and Accountability Analysis of a Secure SMS-Based Mobile Payment Protocol," *Proc. 8th Int'l Conf. Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology* (ECTI-CON 11), 2011, pp. 442–445.
20. *Mobile Payments: Risk, Security and Assurance Issues*, white paper, ISACA, Nov. 2011; www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf.
21. C. Bangdao and A.W. Roscoe, "Mobile Electronic Identity: Securing Payment on Mobile Phones," *Proc. 5th IFIP WG 11.2 Int'l Workshop* (WISTP 11), 2011, pp. 22–37.
22. M. Crowe and E. Tavilla, "Mobile Phone Technology: Smarter Than We Thought," 2012; www.bostonfed.org/bankinfo/payment-strategies/index.htm.
23. J.T. Isaac, S. Zeadally, and J.S. Camara, "A Lightweight Secure Mobile Payment Protocol for Vehicular Ad Hoc Networks (VANETS)," *Electronic Commerce Research*, vol. 12, no. 1, 2012, pp. 97–123.

***Jesús Téllez Isaac** is an associate professor at the University of Carabobo, Venezuela. His research interests include Internet security, performance evaluation of systems, mobile computing, mobile payment systems, and vehicular ad hoc networks. Téllez Isaac received his doctorate in telematics engineering from the Universitat Politécnica de Catalunya, Spain. Contact him at jtellez@uc.edu.ve.*

***Sherali Zeadally** is an associate professor at the University of Kentucky. His research interests include computer networks, network and system security, cybersecurity, mobile computing, energy-efficient networking, and performance evaluation of systems and networks. Zeadally received his PhD in computer science from the University of Buckingham, England. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, England. Contact him at szeadally@uky.edu.*