mobile paymentstoday

Mobile Banking and Payments Security

What banks and payment service providers need to know to keep their customers safe.

CONTENTS

mobile payments today

ROBIN ARNFIELD, writer
robina@networldmediagroup.com

TIFFANY SMITH, custom content editor
tiffanys@networldmediagroup.com

WILL HERNANDEZ, editor, MobilePaymentsToday.com
willh@networldmediagroup.com

NETWORLD MEDIA group

ALAN FRYREAR, chairman
alanf@networldmediagroup.com

TOM HARPER, president & CEO
tomh@networldmediagroup.com

KATHY DOYLE, executive vice president & publisher
kathyd@networldmediagroup.com

Mobile Banking and Payments Security

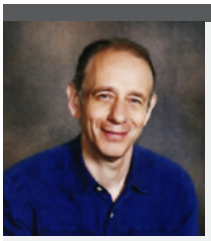
EXECUTIVE SUMMARY

The popularity of banking and online shopping on smartphones and tablets, merchant adoption of mobile point-of-sale (mPOS) devices such as Square and the emergence of mobile wallets and near field communications (NFC) payment services mean that ensuring the security of mobile transactions and the privacy of customers' data is critical.

Mobile devices face the same security risks as PCs and laptops, including malicious apps, viruses and other types of malware and intrusions. However, Dave Jevans, chairman and chief technology officer of IT security firm Marble Security, warns that the security technologies being developed to protect mobile devices are not as mature as the Internet security software designed for PCs.

Internet security firm McAfee Labs collected 2.47 million new mobile malware samples in 2013, with 744,000 identified in the fourth quarter of 2013. The number of mobile banking Trojans — malicious malware programs that steal user credentials — doubled from 1,321 at the start of 2014 to 2,503, reports antivirus firm Kaspersky Lab.

A significant security risk is caused by smartphone users who jail-break or root their mobile devices. This involves a user removing the controls set by the manufacturer of a device so that it can run unauthorized apps, opening the device to the possibility of infection by malware.



Robin Arnfield
Writer, MobilePaymentsToday.com

Robin Arnfield has been a technology journalist since 1983. His work has been published in ATM Marketplace, Mobile Payments Today, ATM & Debit News, ISO & Agent, CardLine, Bank Technology News, Cards International and Electronic Payments International. He has covered the United Kingdom, European, North American and Latin American payments markets.

Guidelines

As a result of the growing number of U.S. consumers who use only mobile devices for banking, the Federal Financial Institutions Examination Council (FFIEC) is expected to issue specific guidance to FIs about m-banking authentication, possibly within the next year. The U.S. banking industry regulator's current Internet banking authentication guidance, which was issued in 2011, is focused on PC banking and needs to be updated in light of the proliferation of mobile banking apps, Jevans said.

In response to the rise of mPOS card readers that attach to smartphones and tablets, the Payment Card Industry Security Standards Council (PCI SSC) is expected to develop specific security standards for mPOS.

Like any merchant who accepts payments cards, mobile merchants using mPOS card readers need to adhere to the PCI SSC's existing data security

standards, the most important of which is the Payment Card Industry Data Security Standard (PCI DSS).

In guidance issued in February 2013, the PCI SSC warned that portable mPOS card readers attached to mobile devices face a threat from fraud specifically because of their mobility. Those card readers can be used not just inside a store but also at remote locations such as customers' homes. One of the risks to the merchant is the ease with which a criminal can steal an mPOS device, modify it to intercept cardholder data and return it without anyone realizing it was gone.

The PCI SSC recommends that merchants using mPOS card readers deploy payment services that offer PCI-compliant point-to-point encryption. That process involves card numbers being encrypted at the point of swiping and being decrypted only by the processor, so the merchant's POS device never has sight of clear-text card data.

Jared Blake, chief technology officer at mobile security firm MokiMobility, believes that the PCI SSC will issue specific PCI standards for mobile merchants within the next 12 to 18 months. "These new requirements will be more stringent than the existing PCI standards that mobile merchants must already comply with," he said.

"These new requirements will be more stringent than the existing PCI standards that mobile merchants must already comply with."

— Jared Blake, chief technology officer at MokiMobility

NFC

According to the Juniper Research report "Mobile Payment Strategies: Remote, Contactless & Money Transfer 2014-2018," the value of m-payments worldwide will rise by nearly 40 percent year on year to $507 billion in 2014. The majority of m-payments transactions take place remotely over the online channel, according to Juniper Research.

Consumer adoption of NFC mobile payments at the point of sale has been hindered by the lack of NFC-enabled smartphones and by the complexity of the commercial agreements needed between banks and mobile telcos to store cardholders' payment credentials in smartphones' secure elements.

As an alternative to NFC, a number of m-payment service providers such as LevelUp and ZNAP offer QR code-based systems that store payment information in the cloud instead of the handset. Starbucks offers QR code-based payments through its mobile app, which had 10 million users in January 2014, but stores its customers' prepaid Starbucks card details in their handsets.

A QR code-based system can be executed on any smartphone, while an NFC-based system requires consumers to have an NFC-enabled phone.

HCE

The recent development of payments industry standards for NFC transactions based on host card emulation (HCE) is expected to provide a major boost for NFC adoption. With HCE, which is supported by Google's Android KitKat 4.4 operating system, transactions take place using payment credentials stored in the cloud instead of on a smartphone's secure element. Consequently, card issuers do not need to rent space in a mobile telco's smartphone secure element.

The SIMalliance, a secure element standards body, is concerned that, because Android is especially vulnerable to mobile malware, HCE implementations on Android devices could be targeted by fraudsters.

"Deploying HCE will require multiple layers of security for HCE-based transactions, such as biometric authentication and the use of tokenization," said Pradeep Moudgal, director of Mercator Advisory Group's emerging technologies advisory service.

Two major smartphone manufacturers, Apple and Samsung, offer fingerprint scanning on their iPhone 5s and Galaxy S5 smartphones, respectively.

Tokenization is a security technology that involves using a one-time number to represent an actual credit or debit card number in a payment transaction. This token has zero value to a criminal, as it can be detokenized only by the tokenization service provider.

Consumer concerns

So far, mobile wallets largely have failed to win mass-market adoption by consumers. According to Michelle Evans, senior consumer finance analyst at Euromonitor, two key reasons for this are consumer concerns about security and privacy.

Deploying technologies such as fingerprint scanning, tokenization and digital identities will help improve the security of mobile wallets and encourage consumer adoption, said Dave Birch, global ambassador at U.K.-based digital payments advisory firm Consult Hyperion.

In its "Recommendations for the Security of Mobile Payments" draft document, the European Central Bank (ECB) says m-payment service providers should provide assistance and guidance to customers regarding the secure use of their services.

CHAPTER 1

Introduction

The mobile phone has evolved from a device used for voice communications and text messaging to a smart computing device that can be used for banking and for remote or point-of-sale payments.

Market research firm Euromonitor estimates that 80 percent of mobile phones sold in the U.S. in 2014 will be smartphones. Over half (59 percent) of mobile phones sold worldwide in 2014 will be smartphones, it predicts.

Mobile banking

The rapid rise in smartphone and tablet ownership has led to a surge in mobile banking usage in the U.S.

“Mobile banking is one of the fastest-growing areas of adoption of technology,” said Ed O’Brien, director of Mercator Advisory Group’s banking channels advisory service.

The first generation of m-banking services was based on SMS messaging, with the second generation using mobile Web browsers. Increasingly, banks have been rolling out mobile apps for smartphone and tablet users.

“Most U.S. banks are providing white-labeled m-banking apps from vendors such as FIS or Fiserv,” O’Brien said. “Their mobile apps offer not just account-to-account transfers but also person-to-person payments and mobile remote deposit capture of checks.”

U.S. m-banking app developer Malauzai Software reported in February 2014 that it was seeing a 4.3 percent growth per month in end-user numbers on its platform. Malauzai provides SmartApps-branded mobile banking apps for credit unions and community banks with assets under $15 billion.

Robb Gaynor, Malauzai’s chief product officer, told Mobile Payments Today in February 2014 that FIs that launched m-banking services using SmartApps in the previous six months saw 15 percent of their customers using SmartApps within 90 to 120 days.

M-banking is expanding rapidly outside the U.S. Two-thirds of the 1,000 Canadians surveyed by Bank of Montreal in August 2013 had downloaded a mobile banking app in the last year, the Canadian bank said.

"There has been a significant rise in m-banking app usage in Canada," said Christie Christelis, president of Canadian research firm Technology Strategies International. "People are getting more confident about using m-banking apps."

The U.K. banking industry has been investing heavily in m-banking and m-payments technology. In April 2014, nine U.K. banks launched Paym, a person-to-person m-payment system that uses mobile phone numbers to identify recipients and eliminates the need for senders to know recipients' banking details. Over 360,000 people registered for Paym at launch, and other U.K. FIs are expected to offer Paym by the end of 2014.

"Nearly all U.K. banks offer m-banking services, some of which provide very sophisticated features such as cardless cash withdrawals at ATMs and person-to-person payments," said Zilvinas Bareisis, a senior analyst at Celent. "The take-up rates and usage levels for m-banking are very high. It's not uncommon for a U.K. mobile banking customer to have over 20 interactions a month with their app."

"Most U.S. banks are providing white-labeled m-banking apps from vendors such as FIS or Fiserv."

— Ed O'Brien, director of Mercator Advisory Group's banking channels advisory service

Mobile payments

While consumers have been quick to adopt m-banking services, m-payments transactions also have been growing. However, consumers still largely use their mobile devices for remote purchases, as NFC-based contactless mobile purchases have yet to see significant traction.

According to "Mobile Payment Strategies: Remote, Contactless & Money Transfer 2014-2018," a report by Juniper Research analyst Windsor Holden, the value of m-payments worldwide will rise by nearly 40 percent year-on-year to $507 billion in 2014. The report found that growth will continue to be driven by remote purchases of physical goods via mobile devices.

Average transaction sizes on tablets already are exceeding those via desktop PCs in many markets, according to Holden. While spending via smartphones is increasing sharply, their primary function in retail is as search-and-discovery devices with the final purchase being made on tablets.

The Far East and China is the largest regional market in terms of m-payment transaction values and is expected to remain so for the foreseeable future.

The Juniper Research report argues that mobile transaction volumes are receiving a significant boost through the adoption of mobile ticketing ap-

plications. Metro and transit authorities in Europe and North America that already have deployed mobile ticketing services are experiencing high levels of adoption.

Slower U.S. growth

In April 2014, IDC Financial Insights published "Business Strategy: Results from the 2014 Consumer Payments Survey," which is based on a survey of U.S. consumers about emerging payment methods. The report says that the growth rate for U.S. mobile payments transactions in 2013 was small compared with growth seen in previous years.

"Mobile payment adoption, after surging in previous IDC surveys, seems to have reached a point of slower growth," IDC Financial Insights said. "Around one-third (37.2 percent) of respondents reported using a mobile payment method of some kind, but that is a relatively modest gain over the last survey. Of those who reported using m-payments, PayPal Mobile is still the most frequently used m-payment method."

PayPal was used by 58.6 percent of respondents in IDC Financial Insights' 2014 Consumer Payments Survey, ahead of both Amazon Payments and Apple's iTunes, which remained at around 40 percent.

mPOS

Mobile point-of-sale (mPOS) card readers that attach to smartphones and tablets no longer are just a tool for micro-merchants to accept card payments. A growing number of large U.S. retailers are equipping their associates with mPOS-enabled mobile devices so they can take payments from customers on the sales floor.

The mPOS solutions that large retailers are installing are more sophisticated than the dongle/card swiper-and-smartphone combinations deployed by small merchants. Provided by vendors such as VeriFone and Ingenico, these solutions offer more than just payments acceptance, with additional features including inventory checking, ordering and product information.

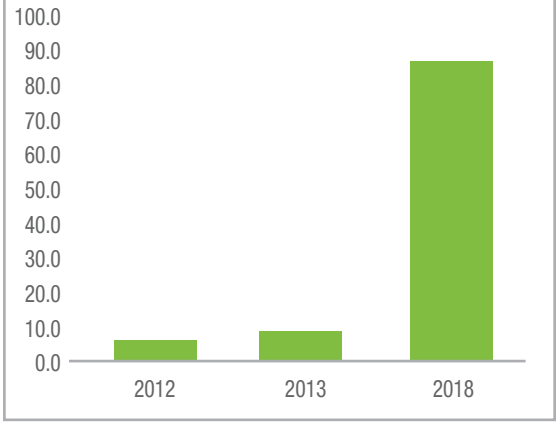
Instead of dongles, large retailers typically deploy either sleeves that encase the mobile device being used as the interface to conduct transactions or integrated solutions that consist of purpose-built, all-in-one mPOS devices.

According to IHS Technology, global shipments of mPOS hardware devices rose by 53 percent to 8.4 million units in 2013 from 5.5 million in 2012. IHS predicts global mPOS hardware device shipments will rise to 88 million in 2018, driven by larger retailer mPOS deployments.

Global shipments of mPOS hardware devices rose by 53 percent to 8.4 million units in 2013 from 5.5 million in 2012.

Dongles were the largest single segment of the mPOS device market in 2013. However, as larger retailers prefer sleeves and integrated solutions that can work with their enterprise resource planning systems, those items will outpace dongles in shipment growth up to 2018, IHS says.

Global Forecast of Shipments of mPOS Hardware (in Millions of Units)



Source: IHS Technology February 2014

NFC

NFC is a set of standards enabling smartphones to exchange payment card credentials, transit tickets, rewards coupons and other information with devices such as POS terminals and contactless card readers using short-range, high-frequency wireless communications. In an NFC transaction, data is exchanged by bringing the smartphone into close proximity or physical contact with the NFC-enabled terminal or reader.

Initial NFC-based m-payment services such as Canadian telco Rogers' Suretap mobile wallet have required payment card credentials to be stored on a mobile device's tamper-resistant secure element. A secure element can be contained in a mobile phone's SIM card, a dedicated security chip that is embedded within a mobile device or a removable microSD card that plugs into the device through a USB port.

In a secure element-based NFC deployment, issuers need to use a trusted service manager (TSM) that provides real-time, over-the-air downloading of customers' card credentials to NFC-enabled SIM cards. A second kind of TSM, known as a secure element TSM, provides encryption and management of card credentials within SIM card secure elements.

From a bank's perspective, the disadvantage of storing the secure element on a SIM card is that the secure element is controlled by the telco, which

will charge rent for storing card credentials on its mobile devices. Storing the secure element on an embedded chip would require the bank to negotiate with the mobile device manufacturer.

As an alternative to NFC, many m-payment players have deployed QR code-based systems that store payment information in the cloud instead of the handset. A QR code-based system can be executed on any smartphone, while an NFC-based system requires consumers to have an NFC-enabled phone, said Michelle Evans, senior consumer finance analyst at Euromonitor.

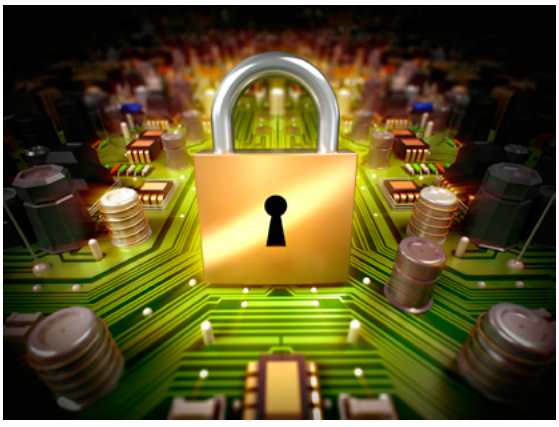
Starbucks and U.S. mobile payments processor LevelUp both use QR codes in their m-payment services. The LevelUp mobile app for iPhone and Android allows registered users to link their credit or debit card to a unique QR code displayed within the app. To pay with LevelUp, users scan the QR code on their phone at LevelUp terminals located at merchants that accept LevelUp.

LevelUp states on its website that no payment card details are stored on customers' handsets. "LevelUp ensures that no live payment data is stored in your phone or delivered to the merchant at any time," it says. When customers sign up for LevelUp by linking their payment card to their QR code, LevelUp does not store the card details on its server. Instead, the card details are stored in a secure vault operated by payments gateway Braintree.

To make a QR code-based m-payment at Starbucks, a customer needs to download an app to his or her smartphone that links the prepaid Starbucks card to the mobile device. Unlike LevelUp, Starbucks stores customers' card details on their handsets.

In January 2014, Starbucks said that it had 10 million m-payment users and that it was processing 5 million weekly m-payments, up from 2 million a week at the end of 2012.

The Merchant Customer Exchange, a coalition of major U.S. retailers, plans to use QR codes in the m-payments platform it is developing.



HCE

The payments industry recently developed standards for HCE-based NFC transactions. With HCE, transactions take place using payment credentials stored in the cloud instead of on a smartphone's secure element. In an HCE transaction, an NFC application running on a smartphone emulates a contactless payment card that is hosted by the issuer in the cloud.

In November 2013, Google added support for HCE to its Android KitKat 4.4 operating system. HCE also is supported by BlackBerry.

In February 2014, MasterCard and Visa both announced their support for HCE. Visa has made available a Visa payWave standard and software development kit for cloud-based NFC payments, while MasterCard has published a specification that uses HCE for secure NFC-enabled m-payments.

According to Juniper Research's Holden, progress in contactless NFC-based m-payments has been slow, with few commercial deployments. However, the medium-term prognosis for NFC payments is now brighter, following the emergence of cloud-based HCE solutions by vendors that offer the opportunity for reduced time to market for NFC services.

"The prevalent business models for NFC have been unattractive to banks and left them dependent on multiple mobile operators, each of which may have its own approach to mobile wallet management," Holden said. "HCE solutions have the potential to revitalize a market which has struggled to gain traction."

Mario Shiliashki, MasterCard's senior vice president of emerging payments, also predicts increased mass-market adoption of NFC due to HCE in 2014.

One of the first retailers to support HCE is North American QSR chain Tim Hortons. In December 2013, Tim Hortons launched an NFC m-payments app based on HCE at its Canadian and U.S. restaurants.

According to a Mobile Payments Today blog post by Cherian Abraham, m-payments adviser at Experian Global Consulting, MasterCard's HCE approach refers to mobile NFC contactless as the only payment modality, whereas Visa envisages augmenting its payWave-based HCE standard with QR and in-app payments in the future.

Abraham said that both Visa and MasterCard's HCE approaches involve using payment tokens. Tokenization is a security technology that involves a one-time number being used to represent an actual credit or debit card number in a payment transaction. In October 2013, American Express, MasterCard and Visa announced a framework for a common global standard for using tokens in online and m-payments.

HCE security concerns

Marble Security's Jevans warned that, if hackers breach the security of a cloud-based HCE system, they will have access to a potentially large number of cardholders' account details.

"There's still a lot of work needed to ensure the security of NFC transactions," Jevans said. "Research into the security of NFC payments is extremely immature, congruent with the lack of adoption of NFC."

"HCE solutions have the potential to revitalize a market which has struggled to gain traction."

— Juniper Research analyst Windsor Holden

A white paper by SIMalliance, "Secure Element Deployment & Host Card Emulation," warns that HCE technology remains immature, unstandardized and, relative to secure element-based deployments, vulnerable to malicious attack.

SIMalliance is concerned about the vulnerability of Android devices to malware, given Google's support for HCE in Android KitKat 4.4. "Given HCE's limitations, SIMalliance considers HCE to be best utilized in cases where stringent security requirements, optimal transaction speeds and always-available functionality aren't mandatory," it said.

"In principle, hardware is more secure than the cloud," said Neil Livingston, director of mobile products at payments processor Carta Worldwide. "Secure elements are designed and tested to a high level by independent labs, so the payments industry should be confident about the security of SIMs and embedded security chips. But, when designed and implemented properly, a cloud-based secure element can deliver effective security to suit the service or purpose for which it was designed."

"There will need to be multiple layers of security for HCE-based transactions such as biometric authentication and the use of tokenization," said Mercator Advisory Group's Moudgal.

NFC handsets

One of the barriers to NFC rollout has been a shortage of NFC-enabled handsets. However, handset manufacturers are addressing this problem.

According to IHS Technology, worldwide shipments of NFC-enabled cellphones rose by 128 percent to 275 million units in 2013 from 120 million in 2012. IHS predicts that NFC-enabled cellphone shipments will rise by over 50 percent year-on-year to 416 million in 2014. From 2013 through the end of 2018, worldwide shipments of NFC-enabled cellphones will rise by 325 percent to 1.2 billion.

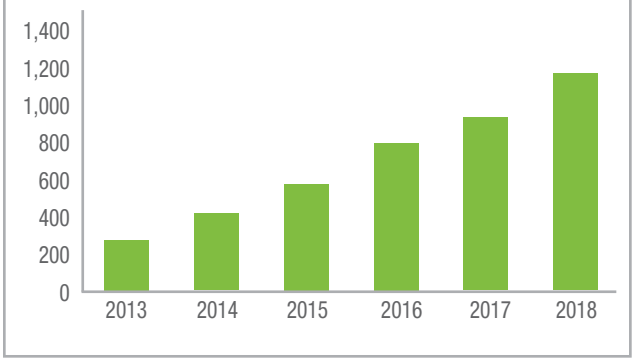
NFC was integrated into just 18.2 percent of the 1.5 billion cellphones shipped worldwide in 2013. In 2018, NFC penetration will rise to 64 percent, IHS says.

"The majority of smartphone makers are adopting NFC wireless communications and payment technology in their products as a de facto standard," said Don Tait, senior financial and ID market analyst at IHS. "Consumers are becoming increasingly aware of the benefits of mobile payment, and NFC wireless [card] readers are proliferating in businesses throughout the world."

"The majority of smartphone makers are adopting NFC wireless communications and payment technology in their products as a de facto standard."

— Don Tait, senior financial and ID market analyst at IHS

World Shipments of NFC-enabled Cellular Handsets (in Millions of Handsets Shipped)



Source: IHS Inc., February 2014

Juniper Research says the opportunity for NFC-based m-payments has been bolstered by contactless infrastructure deployments, since the majority of POS terminals being installed now are shipping with NFC-ready contactless readers.

At the end of Q4 2013, MasterCard had 50 mobile NFC programs live in Europe. In January 2014, Visa had 62 mobile contactless projects live or planned for launch across Europe.

Mobile wallets

So far, mobile wallets have not generated the consumer traction that the m-payments industry had expected.

According to Consult Hyperion's Birch, mobile wallets have failed to win over consumers because of their lack of convenience. "Today's mobile wallets aren't convenient, as users have to do too much to make them work," he said.

Security and privacy concerns also are an issue. "Two major reasons why mobile wallets are struggling to gain adoption are consumer concerns about security and privacy," Euromonitor's Evans said. "M-payments must be as cheap, safe and easy to use as traditional payment methods to even be considered a viable option."

The ECB said in its "Recommendations for the Security of Mobile Payments" draft document that m-payment service providers (MPSPs) should provide guidance to customers regarding the secure use of m-payment services.

"MPSPs should communicate with their customers in a manner that reassures them of the authenticity of the messages received," the ECB said. "They should provide at least one secure channel for ongoing communication with customers regarding the correct and secure use of the m-payment service. MPSPs should inform customers about this channel and explain that any message on behalf of the MPSP via any other means, such as e-mail, is not reliable."

The ECB said MPSPs should initiate customer education and awareness programs to ensure customers understand the need:

- to protect their passwords, PINs, personal details and other confidential data;
- to manage properly the security of the mobile handset by installing and updating anti-virus software and security patches; and
- to be aware of significant threats and risks from downloading software if the customer is not reasonably confident that the software is genuine and hasn't been tampered with.

The ECB recommends that MPSPs set transaction limits for their m-payment services and implement alerts for customers via phone calls, SMS or emails for suspicious or high-risk payment transactions.

Technological developments

Birch believes several technological developments will make it easier to use mobile wallets and consequently help spur wallet adoption.

"HCE, BLE (Bluetooth low energy), tokenization and digital identity standards could really help mobile wallets to take off in 2014," Birch said.

BLE is a proximity communications technology enabling mobile devices to connect to POS terminals and to BLE-enabled beacons that transmit offers to customers. With BLE, mobile devices can be several feet from a terminal or beacon, while NFC requires very close proximity. Apple has developed the iBeacon technology for BLE-enabled beacons that communicate with Apple iOS-based devices.

According to Celent's Bareisis, Apple could offer m-payment services at the point of sale to iPhone or iPad users. IBeacons would recognize Apple users as they entered a store, enabling them to scan goods into a virtual basket and check out remotely using a card registered with their iTunes account, he said.

"With hardware secure element-based NFC, payments companies chose an architecture for proximity payments which is hard to set up," Birch said. "With HCE, retailers and banks can create a mobile wallet interface, and they no longer need to negotiate with a telco over access to the secure element on the telco's SIM cards. Now there's nothing to stop NFC taking off as a convenience rather than a security mechanism."

Birch said that mobile apps can be used to generate single-use tokens that replace card numbers in m-payment transactions. "Tokenization isn't a new idea, but using a mobile app to generate a token means that customer usability issues are no longer a problem with tokens," he said.

Birch believes cross-industry digital identification standards will be key for m-payments. "I don't think banks should create their own identity standards for payments but instead should use the federated identity standards that are being created by industry alliances such as FIDO (Fast IDentity Online)" he said. "A bank server would say to a smartphone: 'authenticate the user of this phone for a payment transaction.' If the phone has FIDO embedded into it, then FIDO will require the user to authenticate themselves — for example, by using a PIN or scanning their fingerprint."

MasterPass

MasterCard is adding support for in-app m-payments to its MasterPass free digital wallet service. MasterPass, which competes with Visa's V.me by Visa offering, allows consumers to store all their payment and shipping information in a single location over the cloud.

"Originally, MasterPass could only be used for in-store or Web-based payments, and now we're enabling consumers to make MasterPass payments for purchases made within a mobile app," said Shiliashki.

MasterPass in-app payments eliminate the need to store payment card credentials across numerous mobile apps, providing consumers with a simplified payment experience, said MasterCard. Forbes Digital Commerce, Fat Zebra, MLB Advanced Media, NoQ, Starbucks Australia and Shaw Theatres Singapore are among the first app providers to offer in-app purchasing capabilities with MasterPass.

"Originally, MasterPass could only be used for in-store or Web-based payments, and now we're enabling consumers to make MasterPass payments for purchases made within a mobile app."

— Mario Shiliashki, MasterCard's senior vice president of emerging payments.

CHAPTER 2

Threats

Mobile devices are subject to the same security threats as PCs, such as malware — software containing malicious code — and vulnerabilities in applications and operating system software that hackers can exploit. A key difference is that the security technologies available to protect mobile users are not as mature as the security software developed for PCs, said Marble Security's Jevans.

Another challenge is the fact that the current generation of mobile devices and their operating systems generally were not designed with payment security in mind, the European Central Bank's "Recommendations for the Security of Mobile Payments" report said.

Mobile malware

Internet security firm McAfee Labs says that in 2013 the growth rate of new mobile malware was far greater than the growth rate of new malware targeting PCs. Mobile malware almost exclusively targets Android devices.

In the last two quarters of 2013, new PC malware growth was nearly flat, while appearances of new Android samples grew by 33 percent, McAfee said in its "McAfee Labs 2014 Threats Predictions" report.

McAfee collected 2.47 million new mobile malware samples in 2013, with 744,000 identified in the fourth quarter of 2013 alone. "Our mobile malware 'zoo' totaled 3.73 million samples at the end of 2013, up 197 percent from the end of 2012," the report said.

At the start of 2014, antivirus firm Kaspersky Lab logged 1,321 unique executables for mobile banking Trojans. A Trojan is a type of malware that, once executed on a PC or mobile device, carries out specific criminal actions determined by the program's author, such as stealing passwords or PINs.

By the end of the first quarter of 2014, the number of mobile banking Trojans logged by Kaspersky had nearly doubled to 2,503, according to its "IT Threat Evolution Q1 2014" report. During the first quarter of 2014, Kaspersky identified 110,324 new malicious programs for mobile devices.

"The majority of the currently available m-banking malware targets Android-based devices," James Walter, manager of the McAfee Threat Intelligence Service at McAfee's Office of the CTO, told Mobile Payments Today. Malware writers target Android-based devices because of Android's open-platform approach and because it has vulnerabilities not shared with other mobile operating systems.

"Mobile malware doesn't affect Apple iOS-based devices to the same extent as Android devices because of the 'walled garden' approach that Apple takes," said BC Krishna, CEO of banking software vendor MineralTree.

"The majority of the currently available m-banking malware targets Android-based devices."

— James Walter, manager of the McAfee Threat Intelligence Service at McAfee's Office of the CTO

Malware growth

Malware can arrive on a mobile device through any of the attack vectors associated with other endpoint devices such as PCs — usually as a downloaded app, but also from visits to malicious websites, spam, malicious SMS messages and malware-bearing ads, McAfee said.

McAfee expects the growth in new mobile malware to continue in 2014. But it also expects to see entirely new types of attacks targeting Android.

"It is highly likely we will see the first real ransomware attacks aimed at mobile devices that will encrypt key data on the device and hold it for ransom," McAfee said in its report. "The information will be released only if the victim delivers either conventional currency or a virtual currency — such as Bitcoin — to the perpetrator. Other new tactics we expect to see in the mobile realm include attacks on vulnerabilities in the NFC features now found on many devices and attacks that will corrupt valid apps to expropriate data without being detected."

"Mobile malware is growing because the criminals go where the money is and where the users are," Marble Security's Jevans said. "All the massive growth in users is on the mobile platforms. Banks are increasingly adopting a 'mobile first' strategy for new development, meaning that the latest and most powerful features in online banking and payments will be offered first on mobile devices and then later on PCs and Macs. This is a real departure from the last 20 years."

Risky apps

In February 2014, Marble Security surveyed over 200,000 Android-based mobile apps in 34 categories for its "Mobile App Threat Report March 2014." The survey found that the riskiest categories of apps are communications apps offering free mobile phone calls or free VoIP (voice over

Internet protocol) calls, followed by social media, news and magazine, and media and video apps.

"Mobile threats are not just about malware," Jevans said. "Even seemingly innocent apps can pose data leak risks as they feed information to advertising engines or hackers' servers and comb through contacts or emails."

Communication apps pose a risk to companies, because they mine the user's contact database. If that database obtains data and updates from a company's active directory of network users, communications apps can mine that data and send it to third parties over the Internet for fraudulent purposes.

Marble Security's analysis of over 4,500 different social media apps determined that this category poses a high risk to companies, employees and individuals.

"There are hundreds of social media apps that expose users and their companies to data loss, account takeover and privacy violations," Marble Security said. "More than 100 social media apps exhibit behavior common to that of malware."

Jevans said that 6 percent of social media apps surveyed by Marble Security read a user's browser history and send it over the Internet. "They know which banking sites the user accesses and where they shop online," he said. "Also, they know the user's email address, which is then used for phishing."

Marble Security found that legitimate m-banking apps — programs provided by banks — generally are well behaved in terms of privacy and security. "However, the security of banking-helper apps provided by third parties that help people log in to multiple banking sites is not good," Jevans said.

Most banks don't recommend that their customers use banking-helper apps, Jevans said. "They pose a security risk as they could send data from the device to a malicious third party. My view is that consumers shouldn't carry out m-banking on a device on which they use social media apps."

Consumers should use only legitimate, trusted apps that they download from their device's app store, Jevans recommended.

Jail-breaking and rooting

Jail-breaking and rooting of smartphones are consumer behaviors that can cause significant mobile security problems, because they open the devices to malware.

Jail-breaking refers to removing the limitations set by Apple in its operating system and running third-party apps that have not been approved by Apple

"Mobile threats are not just about malware."

— Dave Jevans, chairman and chief technology officer of Marble Security.

on an iOS device. Rooting describes the same process on Android devices. Both jail-breaking and rooting break the default security provided by the device manufacturer.

"When you root or jail-break a smartphone, you circumvent the controls," said Jeremy Gumbley, chief technology officer at m-payments gateway provider CreditCall. "This means you don't have to go to the official Google app store or the Apple App Store to get apps, and can install any apps you like."

Gumbley said there is a need for consumer education about the security risks of jail-breaking and rooting smartphones.

"One-tenth of mobile devices in the market have been jail-broken," said Tom Karren, CEO of mobile security firm MokiMobility. "The risk with jail-breaking is that it can lead to a malicious app being installed on the device that spies on the user and steals credentials and unencrypted information."

"If you root a device, anything that happens on that device could be compromised," said Moki's Blake. "For example, if you use fingerprint authentication on a smartphone which has been rooted, then malware could steal a copy of your fingerprint."

Karren said developers can make mistakes that lead to vulnerabilities when they create apps, such as leaving unencrypted customer data on a device, which can be stolen by malware. "Then, if that vulnerable device is jail-broken, it could be hacked, as incorrectly developed apps can leak data," he said.

Marble Security's Jevans said most banks don't write their own mobile apps and instead outsource app development to companies in China and India, for example. "There needs to be security controls for mobile app development such as an audit trail of their SSL (Secure Sockets Layer) encryption and digital certificate validation," he said. Web browsers and apps use digital certificates to certify that a server is secure.

"A common weakness found in m-banking apps is that they lack adequate implementation of SSL or certificate validation, which makes them vulnerable," Jevans said.

In January 2014, Seattle-based security firm IOActive Labs Research revealed in a blog that 40 m-banking apps from the top 60 most influential banks in the world have major security weaknesses. Researcher Ariel Sanchez tested these apps using iPhones and iPads, and found that they all could be installed on jail-broken iOS devices. Most of the log files generated by the apps, such as crash reports, exposed sensitive information that could be used to target users, Sanchez found. Most of the apps also disclosed sen-

"Malware can detect if a smartphone has been jail-broken and then install itself on the phone."

— Jeremy Gumbley, chief technology officer at CreditCall

sitive information through the Apple system log. Seventy percent of the apps did not have any alternative authentication solutions, such as multi-factor authentication, which could mitigate the risk of impersonation attacks.

Also, a new generation of phishing attacks has become popular, in which victims are prompted to retype their user names and passwords "because the online banking password has expired," Sanchez warned. The attackers steal the victims' credentials and gain full access to their bank accounts.

Security measures

CreditCall provides an mPOS payments app and card reader/PIN pad as an attachment to merchants' smartphones.

"When a CreditCall mPOS merchant downloads our mPOS app, we check whether their mobile device has been jail-broken," Gumbley said. "We won't run our software on jail-broken devices."

Moki's managed security service for dedicated mPOS devices such as smartphones and tablets locks down the device so that the only app it can run is an mPOS app. "Our software scans the device's operating system for vulnerabilities and to ensure it has the latest operating system security patches," Karren said. "We also check to see if the device has been jail-broken."

Several third-party software vendors such as Arxan and IBM subsidiary Trusteer offer malware- and jail-break detection tools for mobile devices, which can be provided by FIs to their customers. On its website, Trusteer says its mobile fraud prevention solution provides an accurate and persistent ID that is unique to each device, and identifies device risk factors such as malware infections, rogue apps and jail-broken/rooted devices. The Trusteer software also addresses complex attacks that span both mobile and Web channels — for example, where users' Web banking credentials are stolen and then used on a mobile device to take over the account.

Trusteer leverages a global criminal device database based on fraudulent access detected at its corporate customers. "For both mobile and web-based access, these device risk factors are evaluated by a mobile risk engine to accurately determine login and transaction risk," its website says.

Heartbleed

In April 2014, data security researchers announced that they had uncovered Heartbleed, a website coding error that could allow criminals to steal information protected by OpenSSL security software.

OpenSSL is a cryptographic software library used to authenticate services and encrypt sensitive information. The Heartbleed vulnerability discovered in OpenSSL could allow hackers to decrypt, spoof or perform attacks on network communications that otherwise would be protected by encryption.

"Heartbleed is definitely the most impactful security issue in the short history of the Internet," said Avery Buffington, information security architect at U.S.-based payments processor SecureNet. "The problem is that Heartbleed has the potential to enable hackers to gain access to Web users' sensitive information such as passwords without leaving a trace. This is because data stolen through Heartbleed would not necessarily be reported in a website administrator's log."

Buffington said that it is essential for users to change their passwords and for website administrators to generate new server private cryptographic keys and X.509 encryption certificates. "This is because Heartbleed could expose the server's private key and certificate," he said. "If an attacker has stolen the server's private key and certificate, they could provide a false server site to end users in order to steal their credentials."

X.509 is an industry standard for website encryption certificates.

Reuters cited security researchers as saying that Heartbleed threatens not just website users but also users of iOS- and Android-based mobile devices. The news agency quoted the security experts as saying that iOS- and Android-based mobile apps that use OpenSSL code could be vulnerable to hackers exploiting Heartbleed — for example, if they gain access to the apps through Wi-Fi connections or mobile carrier networks.

Google warned in an April 2014 blog post that Heartbleed affects devices running version 4.1.1 of its Android mobile operating system and that it is distributing patches for the affected version to Android partners.

U.S. financial regulators have taken the threat of Heartbleed seriously. In April 2014, the FFIEC said it expects FIs to incorporate patches on systems and services, applications and appliances using OpenSSL and upgrade systems as soon as possible to address the vulnerability.

FIs should consider replacing private cryptographic keys and X.509 encryption certificates after applying the patch for each service that uses OpenSSL as well as requiring users and administrators to change passwords after applying the patch. The FFIEC said FIs relying on third-party service providers should ensure those providers are aware of the vulnerability and are taking appropriate mitigation action.

"Heartbleed is definitely the most impactful security issue in the short history of the Internet."

— Avery Buffington, information security architect at U.S.-based payments processor SecureNet

The FFIEC noted that server software vendors are incorporating a patched version of OpenSSL into their systems. It recommended that FIs take the following steps:

- Ensure that third-party vendors that use OpenSSL on their systems are aware of the vulnerability and take appropriate risk-mitigation steps.
- Monitor the status of their vendors' efforts.
- Identify and upgrade vulnerable internal systems and services.
- Follow appropriate patch management practices and test to ensure a secure configuration.

Bank Technology News quoted a Citi spokesperson as saying that Citi doesn't use OpenSSL in its standard technology for its retail banking and credit card sites and mobile apps. Bank of America, Capital One Financial, JPMorgan Chase, Citigroup, TD Bank, U.S. Bancorp, Wells Fargo and PNC Financial Services Group have stated publicly that they aren't vulnerable to the Heartbleed bug, Bank Technology News says. Most have said they don't use OpenSSL, the publication reports.

CHAPTER 3

FFIEC Banking Security Guidelines

The FFIEC has yet to provide U.S. banks with specific guidance on security for m-banking. However, industry experts believe the U.S. financial services regulator is likely to issue m-banking security guidance within the next year.

The FFIEC comprises five U.S. Federal Government agencies: the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision and the National Credit Union Administration.

Internet banking guidance

The FFIEC issued its initial guidance to U.S. financial institutions on Internet banking authentication in 2005 and provided an update in 2011. Its 2011 Internet banking guidance said FIs should use multiple layers of authentication involving "the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control."

These controls include fraud detection and monitoring systems that look at customer history and behavior; the use of multi-factor or out-of-band authentication for transactions; and enhanced controls over account activities, such as transaction value thresholds and number of transactions allowed per day.

Out-of-band authentication means that a transaction begun on a PC has to be authenticated using a mobile device. This involves a customer logging on to PC Internet banking and receiving an authentication code on his or her cellphone via SMS.

"All providers of m-banking services should be following FFIEC guidelines for multi-factor authentication," said Mercator Advisory Group's O'Brien.

Mobile-specific guidelines

"There are rumors that the FFIEC will introduce mobile-specific security guidelines within the next year," Danny Piangerelli, chief technology officer at Malauzai Software, said in March 2014. "But there is no mobile-specific

guidance at the moment. Malauzai follows the online banking security guidance that has been issued by the FFIEC."

Piangerelli believes it is only a matter of time before the FFIEC publishes mobile-specific guidance, as mobile is a different channel to the Internet and has unique security challenges.

"Many bank customers now only use m-banking, so their mobile device cannot be the out-of-band authentication method recommended by the FFIEC," said Piangerelli. "This means that m-banking customers don't have an out-of-band authentication method, unless they use an alternative device for authentication."

Marble Security's Jevans warned that, if banks are sending one-time passcodes to a Web banking or m-banking user's mobile device, there is a risk that these passcodes could be intercepted by mobile malware.

"We're seeing more mobile malware that attacks SMS authentication carried out via mobile phones or that acts as fake m-banking apps," Jevans said. "The problem is that SMS isn't a secure, encrypted channel, so malware can intercept SMS mobile transaction authentication messages and send them to a hacker."

In Jevans' view, the FFIEC likely will require layered security for mobile apps in any m-banking guidelines it develops, combining back-end analytics with device risk monitoring and app security scanning.

Piangerelli says Malauzai has systems for authenticating m-banking users by text messages, phone calls or emails. "We can ask a mobile banking user to allow us to call them on a different number or send an authentication code to their PC Internet banking service," he said. "We have methods for shutting off access if a mobile device is stolen and the user reports the theft to the bank."

Banks should ask m-banking users challenge questions — for example, questions about the customer's childhood — O'Brien said, and customers should use only secure networks for m-banking, not insecure locations such as a coffee shop's Wi-Fi network.

"There is a fraud opportunity on an insecure network, as someone could obtain some information about you that they could use in combination with other information about you that they already have to conduct a man-in-the-middle attack," he said. "Even if you're just checking your balance on an insecure network, you could be at risk from someone stealing your credentials."

"Many bank customers now only use m-banking, so their mobile device cannot be the out-of-band authentication method recommended by the FFIEC."

— Danny Piangerelli, chief technology officer at Malauzai Software

A man-in-the-middle attack involves a hacker hijacking communications between a bank website and a customer to carry out fraudulent transactions on the site.

MineralTree's Krishna said that banks offering m-banking applications on the Android platform need to be aware of where the risks originate, so they can implement better risk-management strategies.

"Banks should monitor Android-based accesses more closely," he said. "They should ensure that payment applications and money-movement applications have additional confirmation, and perhaps lower limits. Thirdly, they should encourage customers to use landlines and 'call-to-verify' systems to complete authentication, rather than SMS text messages."

Mobile-ATM integration

A number of banks are introducing services that enable customers to withdraw cash from their FI's ATMs using smartphones. In a mobile-ATM transaction, the customer pre-stages the cash withdrawal by using a mobile banking app on his or her smartphone. Because the app communicates directly with the bank's host system, no card network is involved.

Royal Bank of Scotland (RBS) and its NatWest subsidiary launched a cardless ATM access service for their U.K. customers in June 2012. Customers who use RBS or NatWest m-banking apps can request up to £100 ($168) in cash from the RBS Group's 8,000 U.K. ATMs via their smartphones. They are given a six-digit code to enter into an ATM to release the cash.

Since May 2013, Diebold, U.S.-based processor FIS and mobile wallet app provider Paydiant have been carrying out a pilot with Rosemont, Illinois-based Wintrust Financial Trust of cardless ATM access from Wintrust m-wallets.

In March 2013, the ATM Industry Association (ATMIA) published a best-practice manual for preventing m-banking fraud, placing particular focus on applications linked to ATM systems.

"In a time when the ATM can be used to complete transactions begun on a mobile phone, and as cardless ATM transactions gradually replace ones initiated by plastic cards, it is important to check out any security vulnerabilities associated with mobile phone banking applications," said Mike Lee, the ATMIA's CEO.

CHAPTER 4

PCI

The PCI SSC is an open global forum responsible for the development and management of the PCI DSS and related payment card data security standards. Merchants, processors, payment service providers, issuers, and software and hardware vendors are required to comply with the standards.

The PCI SSC was founded in 2006 by American Express, Discover Financial Services, JCB International, MasterCard and Visa.

The purpose of the PCI standards is to safeguard cardholder data and, in particular, sensitive authentication data by eliminating security vulnerabilities at any point in the payment card infrastructure. The standards cover point-of-sale and e-commerce transactions as well as transactions at ATMs and unattended POS terminals.

Entities that are found to be noncompliant with PCI DSS or that suffer breaches face substantial fines from the card schemes as well as potential liability for the cost of fraud.

"When a mobile device is transformed into a point-of-sale terminal for a merchant to accept card account data, there is a responsibility to protect that information," the PCI SSC says. "Thus, PCI standards begin to apply when a mobile device is used for payment card acceptance."

Mobile merchant guidelines

In February 2013, the PCI SSC issued PCI mobile payment acceptance security guidelines for merchants who use card readers attached to mobile devices to take card payments. Its "PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users" document is intended to educate merchants on the risks that must be addressed to protect card data from exposure when accepting payments via smartphones and tablets.

It is important to note that as yet the PCI SSC has produced only mPOS guidelines, not enforceable standards, for mobile merchants. However, Moki's Blake believes that the PCI SSC will move from guidelines to requirements within the next 12 to 18 months. "These new requirements will be more stringent than the existing PCI standards that mobile merchants

already have to comply with along with all other types of card-accepting merchants," he said.

The PCI SSC warns that, as merchants' mobile devices aren't used solely as POS tools but also to carry out other functions, they introduce new security risks. "By design, almost any mobile application could access account data stored in or passing through the mobile device," it says.

In addition to security risks such as malicious apps, viruses and intrusions, portable mPOS card readers attached to smartphones face a threat from fraud specifically because of their mobility, the PCI SSC says. MPOS card readers can be used not just inside a store but at remote locations such as customers' homes or at farmers markets. One of the risks to the merchant is the ease with which a criminal can steal an mPOS device, modify it so that they can intercept cardholder data and return it without anyone realizing it was gone, the PCI SSC says.

The guidelines have three objectives covering the main risks associated with m-payment transactions:

- Prevent account data from being intercepted when entered into a mobile device.
- Prevent account data from compromise while being processed or stored within the mobile device.

Prevent account data from interception while being transmitted from the mobile device.

Point-to-point encryption

The PCI SSC guidelines recommend that the best option for merchants using mPOS is a PCI-validated point-to-point encryption (PCI P2PE) solution.

The PCI SSC's PCI P2PE standard sets out a specification for the use of strong encryption to achieve point-to-point encryption, where clear-text card data is removed from the payments environment. This is achieved by encrypting data from the point of interaction (where cards are swiped/dipped) until the data reaches the P2PE solution provider's secure decryption environment. By using a PCI-compliant P2PE solution, merchants potentially can reduce their PCI compliance obligations.

"With P2PE, the card number is encrypted in the card reader with a key that isn't known to the merchant and can only be decrypted by the processor or the issuer," said CreditCall's Gumbley.

"Some popular mPOS card readers just convert the mag-stripe data on the customer's card into an audio signal that is transmitted in unencrypted form via the merchant's mobile device," SecureNet's Buffington said. "This is a bad practice, as there could be malware on the device that will intercept the card data. SecureNet's mPOS device encrypts the card data at the point of swipe in the card reader, so the data is encrypted before it reaches the mPOS app on the merchant's device."

Buffington said that, for security reasons, no payments processing should take place on the mPOS device. "It is important that the acquirer or processor's server handles the transaction processing and sends responses back to the mPOS device," he said.

The PCI SSC says that merchants deploying mPOS payments should use a PIN entry device (PED), encrypting PIN pad (EPP) or secure card reader that complies with its Payment Card Industry PIN Transaction Security – Point of Interaction (PCI PTS – POI) standard.

Furthermore, merchants should not implement solutions that permit PIN entry directly into the mobile device. If the system incorporates PIN-entry capability, it should occur only through a PCI-approved PED or EPP, the PCI SSC says.

Merchants should look for an indication of a secure state in their mPOS app — for example, through a displayed secure state icon provided by their app vendor. If no indication is present, the payment app should not be used, the PCI SSC recommends.

Moki says that merchants should check regularly that their mPOS devices have not been physically tampered with — for example, by the insertion of a card skimmer. This check is particularly important where tablets are being used to power self-service kiosks, the company says.

Buffington recommends that small merchants such as coffee shops that use mPOS technology ensure that the Wi-Fi connection they use for their mPOS devices is separate from the Wi-Fi networks they provide for their customers to use while visiting their stores. "The mPOS Wi-Fi connection should be kept on a secure network that is segmented from a public Wi-Fi network," he said.

"Tokenization and point-to-point encryption remove or render payment card information useless to cybercriminals and work in concert with other PCI standards to offer additional protection to payment card data."

— Bob Russo, the PCI SSC's general manager

Mobile software and device guidelines

In September 2012, the PCI SSC published a set of best practices for m-payment acceptance security. The PCI Mobile Payment Acceptance Security Guidelines offer software developers and mobile device manufacturers

Best Practices and Responsibilities

The table below outlines each best practice described within the "PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users" document along with who should be responsible for its implementation. The definitions of those entities that are responsible for the best practices are:

- Merchant as an End-User (M): Any entity that uses the mobile payment-acceptance solution to accept payments.

Mobile Payment-Acceptance Solution Provider (SP): The entity that integrates all pieces in the mobile payment-acceptance solution and is responsible for the back-end administration of the solution. This includes the merchant as a solution provider.

Best Practice	M	SP
1. Prevent account data from being intercepted when entered into a mobile device.	X	X
2. Prevent account data from compromise while processed or stroed within the mobile device.	X	X
3. Prevent account data from interception upon transmission out of the mobile device.		X
4. Prevent unauthorized physical device access.	X	
5. Protect mobile device from malware.	X	X
6. Ensure the device is in a secure state.		X
7. Disable unnecessary device functions.	X	X
8. Detect loss or theft.	X	X
9. Ensure the secure disposal of the device.	X	
10. Implement secure solutions.	X	X
11. Ensure the secure use of the payment-acceptance solution.	X	
12. Prefer online transactions.		X
13. Prevent unauthorized use.	X	
14. Inspect system logs and reports.	X	X
15. Ensure that customers can validate the merchant/transaction.		X
16. Issue secure receipts.		X

PCI Security Standard Council, "PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users"

guidance on designing appropriate security controls to provide solutions for merchants to accept m-payments securely. The document organizes the mobile payment-acceptance security guidance into two categories:

Best practices to secure the payment transaction itself, which addresses cardholder data as it is entered, stored and processed using mobile devices

- Guidelines for securing the supporting environment, which addresses security measures essential to the integrity of the broader mobile application platform environment

Key recommendations include:

- Isolate sensitive functions and data in trusted environments.
- Implement secure coding best practices.
- Eliminate unnecessary third-party access and privilege escalation.
- Create the ability to remotely disable payment applications.
- Harden or lock down supporting systems to prevent unintended access or exposure of a mobile payment transaction.
- Create server-side controls and report unauthorized access.

CHAPTER 5

Mobile Payments Authentication Technologies

M-banking and m-payment service providers have multiple options for authenticating users, including voice or fingerprint biometrics and digital certificates, over and above the standard method of user names and passwords or PINs.

Biometrics

Several major banks are testing biometric authentication for m-banking users.

U.S. Bank announced in February 2014 that it is piloting voice biometrics for mobile login to credit card accounts. Bank employees participating in the pilot use a passphrase such as “my voice is my password” to access their account balances, search transactions and make payments on their accounts in the mobile app.

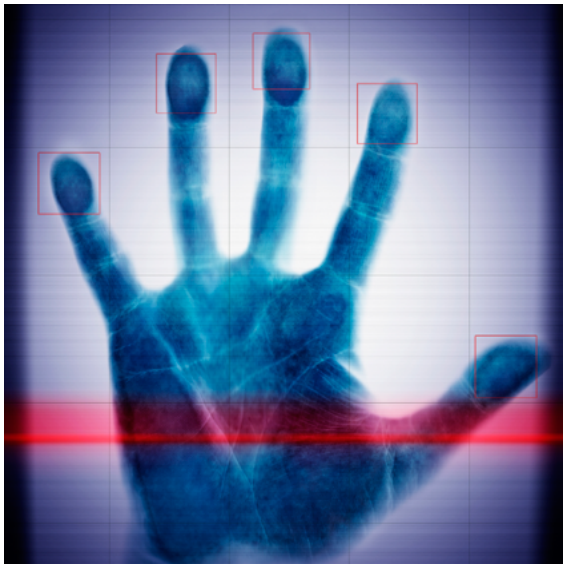
The bank’s voice biometric system, which is supplied by Nuance Communications, replaces PINs, passwords and security questions with voice authentication. The technology can be used with call centers, interactive voice response (IVR) systems, mobile apps or the Web.

“Customers are accustomed to using their voice to interact with their smartphones and can become frustrated with key-entering passwords,” said Dominic Venturo, chief innovation officer at U.S. Bank’s Payment Services. “Exploring a spoken passphrase login through this technology is a logical next step in our work in biometrics.”

Wells Fargo is testing voice recognition for m-banking with its employees, according to The Charlotte Observer. The newspaper reported that Wells Fargo began testing the technology in its m-banking app with employees using their real bank accounts in summer 2013.

Neither U.S. Bank nor Wells Fargo has set a date for customer rollout of mobile apps for voice-recognition login.

Fingerprint scanning



Apple has launched a fingerprint scanner for the iPhone 5s, while Samsung offers fingerprint scanning on the Galaxy S5 smartphone.

"We're starting to see fingerprint scanning on smartphones, but it will be two to three years before this method of authentication becomes mainstream," Marble Security's Jevans said.

In April 2014, Australian bank Westpac's New Zealand subsidiary launched a trial of fingerprint-based mobile banking authentication using the Galaxy S5's fingerprint sensor. Westpac told the Sydney Morning Herald that it soon would be the first bank in the world to let customers log into mobile banking using fingerprint scans.

Westpac uses its New Zealand subsidiary as a testing site for new technologies before launching them in Australia, the Sydney Morning Herald said. When Westpac customers register for fingerprint-based authentication on their smartphones, they will be required to enter their banking user names and passwords and register scans of their fingerprints. Thereafter, they would need to scan only their fingerprint to log in to m-banking.

Initially, Westpac will offer fingerprint authentication on the Galaxy S5, extending the service to other vendors' handsets such as the iPhone 5s.

As yet, Apple hasn't opened up the iPhone 5s's fingerprint scanner to third parties, and it uses the technology only to unlock the phone and to authenticate purchases from its iTunes online store. By contrast, Samsung lets third parties use the Galaxy S5's fingerprint scanner provided that they add its Pass application program interface (API) to their apps.

PayPal

PayPal allows users to log in to its mobile shopping and payments app with their fingerprints using the Galaxy S5's fingerprint scanner. However, in April 2014 the BBC reported that researchers at Berlin-based Security Research Labs (SRL) had managed to fool the Galaxy S5's fingerprint scanner by using a glue-based mold they had created previously to spoof the sensor on Apple's iPhone 5s.

The researchers told the BBC they were concerned that hackers could exploit the flaw in Samsung's fingerprint scanner to fraudulently transfer money via PayPal.

SRL created its hack by lifting a real fingerprint from a smartphone screen and then creating a mold from glue and graphite spray, the BBC said. The result was swiped across the sensor that sits in the phone's home button.

"We're starting to see fingerprint scanning on smartphones, but it will be two to three years before this method of authentication becomes mainstream."

— Dave Jevans, chairman and chief technology officer of Marble Security

PayPal said in a statement that the fingerprint scan unlocks a secure cryptographic key that serves as a password replacement for the smartphone. "We can deactivate the key from a lost or stolen device," it said. "PayPal uses sophisticated fraud and risk-management tools to try to prevent fraud before it happens. However, in the rare instances that it does, users are covered by our purchase protection policy."

Google and SlickLogin

In February 2014, Google acquired SlickLogin, an Israeli company with patent-pending authentication technology that uses sound and mobile phones.

When logging on to a website that runs SlickLogin's software, the user's computer plays a unique sound through its speakers that is picked up and analyzed by an app on his or her smartphone. The phone then sends a signal back to the website to confirm the user's identity.

SlickLogin's technology can be used as part of a two-factor authentication system and could act as an alternative to financial services websites sending one-time passcodes to customers' mobile devices.

Digital certificates

Marble Security's Jevans recommends that m-banking services use the customer's mobile device as a hardware authentication device in itself. "This requires digital certificates and private cryptographic keys that are generated and stored on the device's trusted hardware module and are used in combination with user credentials such as a PIN," he said.

Digital certificates are used to validate an Internet user's identity in combination with a cryptographic key. A trusted hardware module can be either a secure element stored in a mobile phone SIM card or the trusted processing module — also referred to as the trusted execution environment — that resides in a smartphone's main processor chip.

"If the certificate and private key are stored on the mobile device's secure element or trusted processing module, this will provide very strong two-factor authentication for m-banking or m-payment services without needing to use an extra device for authentication," Jevans said. "All Android- and iOS-based devices have the trusted hardware capabilities to securely manage certificates and private keys and ensure that they cannot be copied by a criminal from the device."

Tokenization

According to a white paper by U.S. processor The Member Group, "What

Card Issuers Need to Know about Card-Not-Present Fraud," the use of tokens offers great potential to slow the growth of card-not-present (CNP) fraud in the U.S.

"That's because the tokenization process replaces all of that coveted card account data with a single, secure token," the white paper says. "The token has zero value for a fraudster because it would have to be decrypted by the tokenization provider."

Tokenization replaces the cardholder's primary account number (PAN) with a unique token, and the original cardholder data is stored only on the tokenization system. This process removes a major security burden from merchants, who otherwise would have to face the challenge of securely storing PAN data.

"Tokenization isn't new, as a number of acquirers and processors offer proprietary tokens to merchants for use at the POS," said Dave Fortney, senior vice president of product development and management at U.S. payments network operator The Clearing House Payments Company. "Merchants don't want to store real card numbers, but they want a way of tracking payments for refunds, so the acquirer sends them a token."

What is new is the idea of interoperable, open standards for tokenization, where a consumer receives a token before making a payment at the POS and uses the token instead of a card number.

"These tokens could be used with wearable devices or mobile phones or online," Fortney said.

Several tokenization standards initiatives are underway. In March 2014, EMVCo, the EMV chip card standards body, published "The EMV Payment Tokenization Specification — Technical Framework v1.0". The document is designed to help merchants, acquirers, issuers and mobile and digital payments providers develop globally interoperable tokenization solutions in online or mobile environments.

EMVCo is jointly owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa. Its specification includes data message formats to ensure the interoperability of tokens and outlines the consistent approach that should be used to route and authenticate payment tokens.

In October 2013, MasterCard, Visa and AmEx introduced a proposed framework for a global tokenization standard for digital payments on smartphones, tablets and PCs. By allowing PANs to be replaced with tokens for online and mobile transactions, merchants and digital wallet providers will not need to store customers' card account numbers, the card networks said.

"With tokenization, you can introduce limits to manage fraud detection based on time, location and device. The combination of HCE and tokenization will revolutionize mobile payments."

— Neil Livingston, director of mobile products at Carta Worldwide

To ensure consistency across the globe, MasterCard, Visa and AmEx's proposed standard used to generate tokens will be based on existing industry standards and available to all payment networks and other payment industry participants.

"Once a standard is agreed to and implemented, issuers, merchants or digital wallet providers would be able to request a token so that, when an account holder initiates an online or mobile transaction, the token — not the traditional card account number — would be used to process, authorize, clear and settle the transaction in the same way traditional card payments are processed today," the card networks said. "Tokens can be restricted in how they are used with a specific merchant, device, transaction or category of transactions."

The Clearing House Payments Company

The Clearing House launched a tokenization trial in July 2013 with its U.S. member banks. "We've created a set of specifications which will act as an open standard for tokenization," Fortney said. "The standard needs to be sufficiently flexible to allow issuers to decide who will provide tokenization services for them."

The Clearing House's standard will allow mobile wallets to request or refresh a token and will be able to handle events such as a card being lost or stolen.

"The concept developed by the Clearing House involves dynamic tokens, which would change after every transaction," Fortney said. "As the token would only be valid for a small length of time, it would be of little value to criminals. If malware is used to steal a token from a mobile phone, the token wouldn't be valid."

Card issuers would generate the tokens associated with a user's card number in the Clearing House solution and would maintain the numbers in a data vault. "It wouldn't be possible for criminals to reverse-engineer these tokens, as they would be random numbers," Fortney said.

As not all issuers will want to host their own token vaults, Fortney envisages multi-issuer vaults that could be hosted by processors such as TSYS. "Most U.S. banks already outsource management of their card platforms to processors, so it makes sense that they would outsource the token vaults to them as well," he said. "Major card networks such as Visa and MasterCard would also have vault-hosting capabilities, but maybe the PIN debit networks wouldn't operate vaults."

Consult Hyperion's Birch argued that issuer-based tokenization, where

each issuer has to manage its own tokenization, would involve a lot of work for banks in changing their systems.

"An alternative is network-based tokenization, where tokens are created and managed by the card networks such as Visa and MasterCard, and issuers and acquirers don't have to change their systems," Birch said. "But implementing network-based tokenization will be complicated. A better method may be strong tokenization, which doesn't involve issuers or networks creating a token. Instead, the consumer provides their cryptographically protected digital identity to a merchant, which passes it on to their acquirer. The acquirer looks up the digital identity in a table and sends the transaction to the customer's issuer for authentication."

Fortney stressed that the Clearing House, which processes wire transfers, automated clearinghouse (ACH) and check images, won't be clearing and settling card payments. "We will just provide tokenization services," he said. "The reason we're piloting tokens with mobile devices is that, within 10 years and maybe much sooner, mobile devices will be very relevant in the payments market."

Fortney believes that some form of mobile device ultimately will replace plastic cards. "This device will need to be at least as secure as mag-stripe cards or EMV cards," he said. "Early mobile wallet providers have relied on keeping their users' card numbers on file. Tokenization is a good solution for mobile wallets, as it isn't a good security practice for wallet providers to store their users' card numbers."

Fortney said the Clearing House's member banks felt strongly that the company's tokenization standard shouldn't define what kind of mobile device communication method — such as NFC, QR codes or BLE — should be used.

"The mobile device front-end will evolve quickly, and will standardize eventually, but banks don't want to pick one communications method," Fortney said. "Also, the Clearing House's standard does not dictate what the m-payments authentication method should be — for example, fingerprint scanning."

Authentication levels

Different types of mobile transactions will need different levels of authentication, Fortney said. "Certain functions or purchases levels won't need passwords," he said. "Citi has released a new version of its m-banking app that allows customers to specify that, if they just want to see their balance within the app, they don't need to enter their password."

"To purchase an item in a store such as a pair of shoes, you would need to authenticate yourself using technology such as a fingerprint scanner."

— Dave Birch, global ambassador at U.K.-based digital payments advisory firm Consult Hyperion

Birch agreed that the level of authentication should increase according to the size of the purchase. “If you’re just buying coffee on your mobile phone, you shouldn’t need to authenticate yourself on your mobile phone,” he said. “But to purchase an item in a store such as a pair of shoes, you would need to authenticate yourself using technology such as a fingerprint scanner. For a major purchase using your mobile device, you should be asked additional security questions.”

Zapp

In fall 2014, five U.K. FIs with a total customer base of 18 million — HSBC, first direct, Nationwide, Santander and Metro Bank — will roll out Zapp m-payments for their customers. Zapp will be integrated into the five FIs’ m-banking applications, providing real-time payments between consumers and merchants without the need for digital wallets. Customers will be able to see their bank account balances and select the account they wish to use for the payment.

Zapp payments will generate digital tokens that hide customer bank account details from merchants. The system will work with various POS technologies, including NFC, Bluetooth, QR codes or existing PIN-entry devices.

MagTek

Seal Beach, California-based transaction security company MagTek introduced the Qwick Codes Mobile Wallet in 2012. Qwick Codes are dynamic, one-time-use tokens that can replace payment card information for ATM, POS and online transactions.

The Qwick Codes Mobile Wallet is a subscription-based application that resides in the cloud at Magensa, MagTek's PCI-certified subsidiary. To use the Qwick Codes Mobile Wallet, consumers open the Qwick Codes app, swipe their payment cards through a complimentary MagneSafe reader they receive with a paid subscription and enter the transaction details such as maximum dollar amount and an expiration date. A Qwick Code then is created, which consumers can scan or type into a POS terminal or ATM instead of swiping their cards.

ZNAP

Hong Kong-based MPayMe has developed the ZNAP m-payments platform, which enables consumers to pay via smartphones by downloading an app that links to their prestored credit or debit card and scans merchant QR codes. Transactions are authenticated by entering a PIN, and consumers can redeem coupons and loyalty points that are stored in their ZNAP wallets. ZNAP can be used for mobile POS payments as well as for online transactions.

"In the early days, mobile payments providers put a QR code onto the consumer's handset, which was read by the merchant," said Greg Gresh, CEO of MPayMe's ZNAP subsidiary. "We don't feel this method is totally fraud-resistant. Our method involves the consumer scanning the QR code that is displayed on the merchant's POS terminal. The merchant QR code doesn't contain any sensitive information."

Gresh said that ZNAP's solution operates totally in the cloud and connects to existing payment networks such as Visa, MasterCard or ACH systems. "We don't deliver any sensitive information to the POS terminal or to the user's mobile phone," he said.

In April 2014, international payment processor WorldPay integrated its multichannel payments gateway with ZNAP. First Data formed a strategic alliance in May 2013 with MPayMe to act as exclusive distributor of ZNAP in Asia-Pacific.

FIDO

The FIDO (Fast IDentity Online) Alliance is developing open standards to address the lack of interoperability among strong online and mobile authentication technologies and to remedy the problems users face with creating and remembering multiple user names and passwords.

Strong authentication is identified as the combination of two or more factors of authentication:

- Something the user knows (e.g., user name and password)
- Something the user has (e.g., a mobile device, smart card or a one-time passcode calculator)
- Something the user is (e.g., a biometric such as a fingerprint or face scan)

FIDO says its digital identity standard will enable users of online, cloud and mobile applications to access services and confirm transactions with authentication methods that are more secure, more private and easier to use than passwords and PINs.

FIDO's protocols use standard public key cryptography techniques for authentication. Public key cryptography is an encryption method that is used to verify an identity or to encrypt data or messages.

FIDO says its open specifications will support a wide range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, and security solutions and communications standards such as encryption chips embedded in mobile devices; USB-based security tokens; embedded secure elements; smart cards; BLE; and NFC.

USB-based security tokens provide secure storage for multiple login credentials, so consumers need to remember only a single password or PIN to access a system or authenticate a transaction.

Several technology vendors are developing FIDO-ready authentication services, including Samsung, PayPal, AGNITiO, Go-Trust, Infineon Technologies, Nok Nok Labs, NXP Semiconductors and Oberthur Technologies.

Samsung's Galaxy S5 smartphone uses FIDO software in combination with its fingerprint scanner to authenticate PayPal m-payment transactions in the cloud. PayPal says it provides a secure cloud-based wallet and does not store personal information on the mobile device. The only information the device shares with PayPal is a unique encrypted key that allows PayPal to verify the identity of the customer without having to store any biometric information on PayPal's servers.

AGNITiO has developed FIDO-based Voice iD, which uses natural voice recognition to replace passwords and PINs when authenticating smartphones, laptops and applications and securing digital transactions. Go-Trust has developed a FIDO-ready microSD card that contains 8 gigabytes of storage and can be used for secure, FIDO-compliant login on laptops, PCs and Android devices.

GLOSSARY

Bluetooth: Wireless protocol using short-range communications technology to facilitate data transmission over short distances.

Cryptography: An area of computer science dealing with encryption and authentication. In applications and network security, it ensures access control, information confidentiality and integrity.

Digital certificate: An electronic document that uses a digital signature in combination with a public key as proof of identity of an individual user or a server connected to the Internet. See “public key.”

EMV: The EMV (Europay, MasterCard and Visa) chip card standard is designed to prevent card skimming and counterfeiting, as EMV-compliant cards contain an embedded microprocessor as well as a magnetic stripe.

Encrypting PIN pad (EPP): A tamper-responsive security device that provides secure PIN entry and storage of cryptographic material. It is used in ATMs and self-service POS terminals.

Encryption: The process of converting information into an unintelligible form that can be deciphered only by holders of a specific key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure. See “strong cryptography.”

Encryption algorithm: A series of instructions used to change unencrypted data to encrypted data, and back again. See “strong cryptography.”

Hardware security module (HSM): A physically and software-protected cryptographic device that provides a secure set of cryptographic services, including the supply of keys as well as encryption, decryption and authentication.

Jail-breaking: The rendering of a cellphone such that it is no longer subject to the limitations originally imposed on it by its manufacturer. Jail-broken mobile devices allow access to their proprietary operating system, which then allows the installation of third-party applications not released or controlled by the manufacturer or proprietor. See “rooting.”

Key: A value that determines the output of an encryption algorithm when transforming plain text to ciphertext. The length of the key generally determines how difficult it will be to decrypt the ciphertext in a given message. See “strong cryptography.”

Key management: A set of cryptographic processes and mechanisms that support key establishment and maintenance, including replacing older keys with new keys as necessary.

Near field communication (NFC): A short-range, wireless RFID (radio-frequency identification) technology that uses interacting electromagnetic radio fields instead of the typical direct radio transmissions. See ISO/IEC 18092 for specifications.

Payment Application Data Security Standard (PA-DSS): The PA-DSS assesses ATM and POS applications software to ensure they support PCI DSS compliance.

Payment Card Industry Data Security Standard (PCI DSS): A standard created by the Payment Card Industry Security Standards Council (PCI SSC) that applies to all entities such as FIs, retailers, payment service providers and merchants that process, store or transmit cardholder data. Entities that are not compliant with PCI DSS run the risk of losing the ability to process payments and may be fined. PCI DSS requires an organization to have security policies and programs in place to protect the cardholder data it stores.

PCI PTS (PIN Transaction Standard): This standard applies to manufacturers of POS terminal PIN entry devices (PEDs), encrypting PIN pads (EPPs) on ATMs and self-service POS devices, and hardware security modules. HSMs are systems used by processors to create cryptographic keys for ATMs and payment terminals. Manufacturers must ensure their devices comply with PCI PTS requirements, and merchants must deploy PCI PTS-compliant devices. PCI PTS has three elements: PCI PTS – POI (Point of Interaction); PCI PTS – HSM; and PCI PTS – PCI PIN Security.

Private key: The secret component of an asymmetric key pair. The private key always is kept secret by its owner. It may be used to digitally sign messages for authentication purposes, and it may be used to decrypt messages encrypted with the matching public key.

Public key: The public component of an asymmetric key pair. The public key usually is publicly exposed and available to users. A digital certificate to prove its origin often accompanies it. It may be used to validate a message signed by the matching private key, and it can be used to encrypt messages to be sent to the private key holder.

Public key cryptography: An encryption method that is used to verify an identity or to encrypt data or messages. It consists of two keys: one public and one private. The public key is in the public domain and available to all users, and the private key is kept secret. Public key cryptography also may be used to verify digital signatures to authenticate the message sender.

Rooting: Gaining unauthorized administrative control of a computer system. See “jail-breaking.”

Secure Digital (SD) card/MicroSD card: A nonvolatile memory card format used as additional memory for mobile devices.

Secure element: A formally certified, tamper-resistant, stand-alone integrated circuit often referred to as a "chip."

Strong cryptography: Cryptography based on industry-accepted algorithms, along with strong key lengths and proper key-management practices. Industry-standard encryption algorithms include AES (128 bits and higher), Triple DES (minimum double-length keys) and RSA (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

Triple DES: Triple Data Encryption Standard.

Trusted service manager: A TSM acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, mobile device manufacturers or other entities controlling the secure element on mobile devices. The TSM enables service providers to distribute and manage their contactless applications remotely by allowing access to the secure element in NFC-enabled handsets.

Sources: EMV Migration Forum, European Central Bank, PCI Security Standards Council

REFERENCES

"Business Strategy: Results from the 2014 Consumer Payments Survey"
By James Wester, research director, Global Payments Team, IDC Financial Insights
http://www.idc.com/getdoc.jsp?containerId=FI247805

"Balancing mobile payments security vs. ease of use"
Mobile Payments Today
http://www.mobilepaymentstoday.com/blog/11611/Balancing-mobile-payments-security-vs-ease-of-use

"EMV Migration Guide"
By Robin Arnfield, Networld Media Group
http://www.networldmediagroup.com/inc/sdetail/8593/17226

"EMV, PCI and the ATM Industry"
By Robin Arnfield, Networld Media Group
http://www.networldmediagroup.com/inc/sdetail/8593/17477

"FFIEC may be prepping guidance for mobile banking"
Mobile Payments Today
http://www.mobilepaymentstoday.com/article/216883/FFIEC-may-be-prepping-guidance-for-mobile-banking

"IT threat evolution Q1 2014"
Kaspersky Labs
http://www.securelist.com/en/analysis/204792332/IT_threat_evolution_Q1_2014

"The MPOS Impact: The Shifting Balance of Power"
Mobey Forum white paper
http://www.mobeyforum.org/whitepaper/the-mpos-impact-the-shifting-balance-of-power/

"Mobile payments taking off in the UK"
Mobile Payments Today
http://www.mobilepaymentstoday.com/article/229771/Mobile-payments-taking-off-in-the-UK

Mobile payments security white papers
Mobile Payments Today
http://www.mobilepaymentstoday.com/whitepapers/industry/30/Security

"NFC Forum publishes new specifications"
Mobile Payments Today
http://www.mobilepaymentstoday.com/article/231161/NFC-Forum-publishes-new-specifications

NFC Forum
http://nfc-forum.org/

OpenSSL "Heartbleed" vulnerability alert
Federal Financial Institutions Examination Council
https://www.ffiec.gov/

"Recommendations for the Security of Mobile Payments" draft document
European Central Bank
https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftp-c201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9

"Secure Element Deployment & Host Card Emulation v1.0"
SIMalliance
http://www.simalliance.org/en/se/se_marketing/

"The iBeacon/BLE vs NFC Debate: Now the Truth"
Mobile Payments Today white paper sponsored by Pyrim Technologies
http://www.mobilepaymentstoday.com/whitepapers/7689/The-iBeacon-BLE-vs-NFC-Debate-Now-the-Truth

The Payment Card Industry Security Standards Council
https://www.pcisecuritystandards.org/security_standards/documents.php

"What Card Issuers Need to Know about Card-Not-Present Fraud"
By Nicole Reyes and Brandon Kuehl, The Members Group
themembersgroup.com/CNPfraud

"Who's Watching You?"
McAfee Mobile Security Report, February 2014
McAfee Labs
http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf