AMERICAN BANKER
On Focus and In Depth

COVER STORY

As Mobile Banking Grows, So Do Security Fears

American Banker | Thursday, December 9, 2010

By Karen Epper Hoffman

Mobile banking has matured from a cutting-edge technology to one that's seen as a necessity in almost every bank's toolbox.

But at the same time, malware, phishing, social engineering and data attacks on the mobile platform and on mobile-banking services are becoming more prevalent. Industry experts say that these attacks will continue to grow as this delivery channel becomes a larger, richer target with more U.S. consumers using it to gain access to financial information and conduct transactions.

Cases in point: In July, **Citigroup Inc.**'s mobile banking application for iPhones was found to have a security flaw where user account information could be backed up and saved to a hidden file on the owners' handsets. Fraudsters are coming at mobile banking users through text, too — customers of several community banks and credit unions were targeted in voice- and text-based phishing scams last summer.

Even more recently, in early November, the security research firm **viaForensics** announced that it had found flaws in mobile applications from **Bank of America Corp.**, **USAA**, **JPMorgan Chase & Co.**, **Wells Fargo & Co.** and **TD Ameritrade**, according to reports published in CNET and *The Wall Street Journal*. The security researcher discovered, for example, that USAA's Android app stored on the phone copies of Web pages a user visited and that Wells Fargo's Android app stored user name, password and account data in plain text on the phone. (Wells Fargo, like other banks, frequently monitors its mobile applications for security problems and corrected the problem almost immediately, according to bank spokeswoman Michele Scott.)

As mobile banking matures into much more than an extension of online banking — most banks still require mobile users to first be online banking customers, though this is changing at institutions like Wells Fargo and **Patelco Credit Union** — banks must expand beyond conventional security measures. Traditional methods of authentication used in online banking will not cut it for mobile banking, according to a Javelin Strategy and Research report issued in October.

"So far, we've really found mobile security to be wanting," said Robert Vamosi, an analyst at Javelin in Pleasanton, Calif. "There's been a lot of focus on [consumer] adoption and not enough specific[ally] on security." He said that, though the ability to download applications is drawing more retail consumers to use their phones for data services like banking, many people get lulled into a false sense that any application they might see with a bank's application, no matter where they see it, is legitimate.

For banks and their customers, providing solid security while keeping mobile services convenient and also conveying a sense that users are protected is quite a juggling act, one that most banks are figuring out as they go along. Some banks, particularly those that got into mobile early, as Wells Fargo did, have been "ramping up slowly," Vamosi said. "Wells had mobile for a while and didn't advertise it; … they would build and monitor. They're doing it in measured steps."

Up until recently, the saving grace that had limited fraud in mobile banking was that the market was not big enough to target, executives say. The mobile platform as a whole was plagued by 516 pieces of malware last year, compared to more than a million malware threats found in the ubiquitous Windows platform, according to Markus Jakobsson, a well-known computing security expert and co-founder of the start-up FatSkunk.

"It's been small, but it's evolving quickly. Malware authors are good businessmen," Jakobsson said.

When it comes to mobile software, said Teddy De Rivera, executive vice president of the Internet services division at Wells, it is important for banks like his not only to vet their applications but also to convey to their customers that they should be cognizant of what they download and from where.

"We've got our fraud information center," De Rivera said. "It goes to our advantage to make sure that we have more educated customers. … That's true in the physical world as well."

"The cybercrooks are going where the money is," said Anthony Vitale, an assistant vice president of information technology development at Patelco in San Francisco. "Now that mobile [banking] is becoming so pervasive … now that the money's there, that will be motivation for the hackers to develop malware."

It's Complicated

However, securing the mobile channel is not simply a case of been there, done that. Though possibly more promising in its scope than online banking, mobile access also raises several unique security challenges.

First, the mobile banking ecosystem itself is far more complex than online's. Banks, carriers, application developers, platform developers, handset manufacturers and chip makers are all participants in this massive food chain. This can not only complicate matters in terms of setting (or marrying) security standards but also create a wide degree of variance in terms of security.

For example, some analysts like Vamosi say that open-source applications for smartphones, like those that can be downloaded from **Google Inc.**'s Android Market are less secure than the "walled garden" created by the Apple Store, where all applications must be certified by **Apple**.

"These newer phone applications, where are they all coming from?" said Paul Schaus, an analyst at CCG Catalyst in Phoenix. "Banks and their vendors have to be one step ahead, and in this world, that's hard to do."

Last December, malware masquerading as applications for more than 50 banks that did not have mobile applications was discovered in the Android Market. Android, BlackBerry and iPhone have all since made commitments to test all their apps for authenticity or even, as BlackBerry does, require application developers to buy license keys to further authenticate their applications. Though smartphones still hold a minority share in the U.S. marketplace, most industry observers point out that smartphone users are the most apt to be early adopters of mobile banking.

Though they are working separately toward strong and consistent security requirements, carriers and banks do not necessarily work closely together on specific security implementations. "We have limited interactions with the telecoms and the handset manufacturers," says Todd Inskeep, an authentication and customer protection executive at Bank of America, which offers mobile banking through mobile Web, applications and, most recently, text.

"There are no hard and fast regulations [regarding mobile banking] on the carriers themselves and how they embed security," Patelco's Vitale says.

The mobile phone as a banking platform also presents security challenges based on how consumers use it. Because many people carry their cell phones with them virtually everywhere, there is a greater risk of loss than would typically be the case with a personal computer. "It's surprisingly common to forget your handset," FatSkunk's Jakobsson says. "The number of lost devices is high. And people often store their passwords [for mobile banking and other services] on there, too."

Indeed, mobile users have become accustomed to carrying a wealth of sensitive information, including financial passwords and data, on their cell phones. Many smartphone users also have taken to connecting to the Internet using free Wi-Fi hubs, which can expose them to man-in-the-middle attacks and malware, according to Vamosi.

"The mobile device is inherently vulnerable because it can be lost or stolen," Vitale said, "and the proliferation of wireless hotspots … leaves those users open."

Marc Warshawsky, a mobile channel planning executive at Bank of America, says that on the Web site and in other communications, his bank tells its more than 5.5 million mobile banking customers not to store any sensitive financial information on the phone, in order to mitigate the risk if the phone is lost or stolen. And on the upside, he pointed out that, owing to the fact that consumers are so dependent on their mobile devices, "people notice their phone being lost very quickly."

Different Approaches

Mobile banking is further complicated by the fact that banks and their customers may be interacting through the mobile Web, downloadable applications or text — three modes of communication with three sets of security concerns. More and more banks are offering mobile banking through two or three of these mobile paths and, therefore, must tailor secure technologies, procedures and capabilities for each.

Downloadable applications offer banks the ability to build a branded, customized experience for customers that can allow for more complex transactions to take place more easily. Though the apps are limited to smartphone users, this group is one that has tended to embrace mobile banking early on. Though **Huntington Bancshares Inc.** already offers mobile banking via text or mobile Web, the Columbus, Ohio, bank will roll out applications for iPhone and Android in early 2011, according to Jeff Dennes, a senior vice president and the director of online and mobile services at Huntington.

"The app world is something that didn't exist two years ago," Dennes said. But by September, Apple device users had downloaded more than 6.5 billion applications from Apple's App Store alone. Dennes, previously an executive at USAA, said he hopes that offering the downloadable application will mean better opportunities for two-factor authentication than is possible through other means. [It is difficult to verify the sender of a text message; and unlike the static online experience, IP addresses in mobile are fluid because browsers are literally on the move.] One-time passwords, virtual tokens and other authenticating technology are all being considered, he added.

In the PC-based online world, Bank of America offers customers free access to McAfee antivirus software for a year, as an encouragement to protect their own systems, according to Inskeep. A similar offering might be made on the mobile platform if the threat there increases. "Malicious software is a big deal," he said.

Bancorp South offers mobile access solely through downloadable application, which customers can use to check balances, transfer funds between accounts and even pay bills, according to Michael Lindsey, a senior vice president and the retail banking division head at the Tupelo, Miss., bank. Bancorp South's approach has been focused largely on password entry, but Lindsey said that, as the bank eventually expands the options for functions customers can perform, it may adopt the use of encryption tokens.

Text is becoming an increasingly popular mode of access because it does not require a smartphone and the use of text has surpassed making voice calls among many younger cell subscribers. But text has its drawbacks as well. Arah Erickson, the senior vice president for retail mobile banking at Wells Fargo, pointed out that, with text, the data is not encrypted and can easily be exposed to access. As a security precaution, banks like Wells and Huntingon limit the information sent on this channel solely to alerts or information that does not include account numbers.

"People are doing different things in text than they would in downloadable apps," Erickson said. "Complex money movement over text isn't going to happen."

Javelin's Vamosi said that one of banks' best security measures is to consider carefully what functionality they offer based on each modality's strengths and weaknesses. "You need to treat text and mobile Web differently," he said. "Text is the weakest; … you should not expose sensitive information over there. And the mobile browser is not as sophisticated" as PC browsers.

For the moment, many banks are carrying over the security technologies and protocols that have worked in online banking to mobile. Though aware that mobile banking is increasingly breaking free of simply extending online services, banks hope that these will provide a foundation upon which they can build. Wells' De Rivera says, "We're leveraging a lot of the same tools in the mobile channels, even though customers approach it differently and have different needs."

Behind-the-scenes technology like device recognition and pattern recognition (on transactions or even behavioral profiling) are coming more into play as banks strive for subtle ways to verify users' identity without putting up too many barriers to use. Inskeep said that Bank of America, for example, is using its SiteKey image-based authentication — initially used to validate online banking customers — for mobile banking because it also supplies a "consistent experience" for customers across platforms.

Banks are also making sure to underscore their consumer protections in order to reassure customers that, fraud or no, they can trust their bank to back them up. "Security is always top of mind for us, but we don't want to make it such that consumers can't use the service," said B of A's Warshawsky. "We offer the same zero liability through the mobile channel [as other delivery channels]. … If a customer reports fraudulent activity, we're going to cover them."

Ultimately, getting to a more secure mobile banking platform is a work in progress — and a convoluted task at that. Though most bankers were loathe to share specifics about their security measures, most agreed that, even more so than with online, mobile banking would require a layered approach to security. This incorporates authentication technologies that are transparent to the user — checking the device or the handset chip and looking for patterns, behavior, geolocation or even IP address where it makes sense — as well as customer-facing authentication and parameters regarding transactional capabilities and access to accounts.

"There are so many opportunities to further enhance other channels through mobile," Wells' De Rivera said. "In understanding mobile, we need to think of this [environment] as not being static but dynamic."

Karen Epper Hoffman, a former American Banker technology reporter, is a freelance writer in Poulsbo, Wash.