

Security's Role in Deploying Transaction-Enabled Mobile Applications

Executive Summary

Companies recognize the value brought by moving transactions to the mobile channel. A number have already done it, but a lot more plan to do so within the next 12 to 24 months. And many plan to expand the number of applications as well. Nevertheless, only a small portion of companies offer the same transactions on mobile platforms as those services that are currently enabled on their Web sites.

Firms recognize the barriers to rolling out mobile applications. These barriers naturally include infrastructure and business issues, but the overriding concern resides around security. In fact, security of mobile transactions is perceived to be so important that organizations give weight to this in their marketing messages.

Examining the security issue more closely, authentication is one of the greatest concerns. Regardless of whether an organization has experience in deploying transactions via mobile applications, authentication is seen as a prime challenge to resolving security issues. And even for those with experience, it is the number-one challenge – and it seems to grow as an organization's experience in this environment increases.

To capitalize on the promise of the mobile channel to support applications, organizations must solve the user authentication problem – and they must do it in a way that is economical and easy for users.

The rapid growth in the use of smartphones and sophisticated mobile devices, combined with growing user expectation of accessing information and doing business anywhere and anytime, is spurring demand for mobile applications that incorporate transactional features, particularly ones that replicate the online experience. One of the first steps in this direction is simply to enable a mobile device to access existing Web applications; the next step will be to develop applications for the mobile devices themselves.

With strong customer demand, companies that have traditionally provided transactional-based services online have great incentive to develop and support mobile transaction applications. However, extending these services to the mobile environment brings a new set of challenges. Notably, companies must secure their applications and associated data, develop the applications for a wide range of devices and make them easy to use, and address and allay customer concerns about transaction security.

To better understand these issues and get a clearer picture of the state of the mobile transaction applications market, and the role of security within that market, Ziff Davis Enterprise conducted a survey of application developers and architects involved with their firms' strategies to deliver mobile applications to external users (see: Survey Methodology sidebar on page two).

The study asked about current and planned mobile transactional application deployments, which transactional functionality was in demand and being made available to mobile users, and what the obstacles were in deploying these applications.

Transition to Mobile

Most organizations (as many as 80 percent of those surveyed) offer online transactions of some sort for users who come to their Web sites. Providing or updating account or personal information is the most typical transactional feature currently offered, but account management and mobile payment also are common.

However, many organizations currently do not extend this functionality to mobile users. And quite interestingly, there is a direct correlation between the number of mobile applications currently offered and the functionality extended today.

On average, firms with transactional mobile applications only make 31 percent of their total online transactional capabilities available today via the mobile channel, making 69 percent of the functionality unavailable to mobile users. Worse, half of the companies that support only a few mobile applications (four or fewer) say 10 percent or less of their online transaction functionality is available through mobile applications.

From a user's perspective, this is quite a noticeable limitation. People used to freely accessing account information, transferring funds, checking order status, or selecting and buying products online might be discouraged if they try to duplicate their online activities from a company's mobile application.

Conversely, companies that have embraced mobile applications and offer more of them (four or more) tend to make more functionality available through these applications. For instance, about a quarter of these companies make 50 percent or more of their online transaction functionality available through their mobile applications. Even so, there is still only a small percentage of these organizations that extend financial transactions (e.g. making payments, depositing, or withdrawing or transferring funds) to the mobile channel.

As we shall see, a possible explanation for the disparity in the percentage of transactional functionality that is offered to mobile users is that organizations lack the appropriate experience to support this endeavor. In particular, many find it hard to extend capabilities they offer online to the mobile channel – and more importantly, to extend them securely. Those who offer and support many mobile applications likely understand the challenges, and have developed solutions and methods to address them. Those who do not have the appropriate expertise or have not discovered the right solutions simply have chosen not to open up access, or are severely limiting access to transaction capabilities through mobile applications.

Market Poised for Growth

Still, many firms are planning to add mobile transactional applications in the near future. Among firms with no current transactional mobile applications, about half expect to deploy at least one with transactional functionality within two years. One of the first steps in this direction is for these organizations to enable a user's mobile device to access their existing Web applications to perform transactions; the next step will be to develop applications for the mobile devices themselves.

Drilling down a bit further, the survey found that almost 40 percent of the firms that do not currently offer such applications plan to offer some within the next 12 months. An additional 12 percent plan to offer them within the next two years.

Moreover, companies that already offer mobile transaction applications plan to introduce more of these applications, and expect to make a higher percentage of their online transaction capabilities available to mobile users.

What's driving the interest in this arena? Not surprisingly, the main reason companies want to develop mobile transaction applications is to make their customers happy. About 55 percent of the survey respondents

Survey Methodology

This study on transactional mobile applications was carried out by Ziff Davis Enterprise (ZDE) in conjunction with the independent research firm The Strategy Group. To collect data, an online survey was carried out from December 18, 2009 to January 13, 2010, using a random sample of IT buyers from the ZDE database. These managers worked in firms with 100 or more employees, and were involved in their firms' strategies to deliver mobile applications to external users. The study was then extended by conducting additional surveys to companies of all sizes. In total, 287 qualified respondents completed the survey.

said convenience to customers was a stimulating factor for the development of mobile transaction applications. About 30 percent noted that an additional driver was that mobile applications enabled more or better contact with the customer. Customers appear to be demanding this, too. Over 20 percent of those surveyed acknowledged that high customer demand was a factor behind their interest in deploying these transactions via the mobile channel. Organizations clearly perceive this as a differentiation from their competitors.

The evolution of the mobile environment, with more robust mobile devices and wireless technologies, lower infrastructure costs, and easier development of applications is providing a further stimulus. The newer generation of mobile devices (and notably smartphones) is now finally able to support comparable functionality to what previously had only been offered online. This greatly expands the potential market for mobile transaction applications.

Finally, a surprising number of companies – more than 20 percent of those surveyed that have already deployed a number of mobile applications – have recognized an opportunity to enhance security by using the mobile channel for transactional applications. This could be because of perceived opportunities to use the mobile channel as a security option for online transactions.

Providing Security is a Key Obstacle to Deployment

With the aforementioned great interest in offering more mobile transaction applications, the question becomes, what is holding companies back?

When asked about obstacles to deployment, security was the top concern among those surveyed, regardless of whether or not the

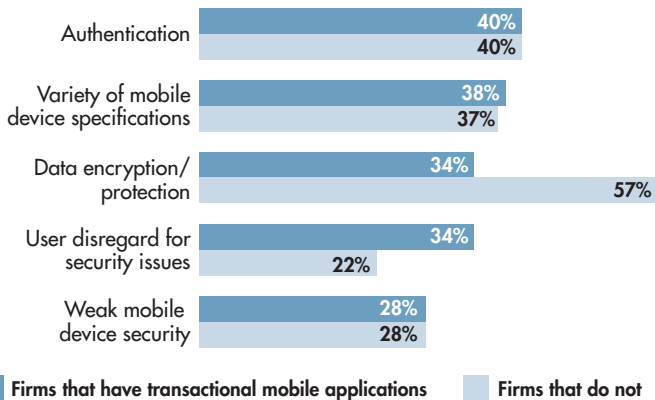
organization had deployed any transactional mobile applications. More than 50 percent of organizations that had not deployed such applications ranked it as one of their top three concerns, and over 40 percent of those that had deployed these applications continued to rank it as a key concern.

Other concerns noted by survey respondents were related to issues such as the costs of development, resources required for developing or maintaining the applications, and various business concerns, such as compliance issues.

Under the umbrella of security, however, the survey pointed to a broad range of underlying issues that are obstacles to further deployment. These ranged from concerns about data encryption and protection, authentication, and the weakness of mobile device security features, to more general concerns such as the disregard for security issues by users.

Organizations clearly recognize the perceptions around security, and the potential impact with users. Fifty percent of those that have already deployed transactional mobile applications factor the security message very prominently in the messaging around their products and services.

Challenges in Providing Security for Transactions Made Via Mobile Applications



Understandably, respondents to the survey noted that failing to address some of these issues would inhibit their customers from performing transactions via a mobile application. And while some of these hurdles (such as slow transactions speeds) are largely beyond the control of many organizations, other challenges (such as the storage of sensitive data or transaction security) can be addressed in the development of the application and the security that surrounds it. As an example, stored data or data in transit can be safeguarded by encryption, and unauthorized access to accounts can be handled through stronger authentication.

But the survey also revealed that organizations recognize the challenges in addressing some of these issues, and therefore their ability to exploit the mobile channel. In particular, those surveyed consider authentication to be one of the top three challenges in providing security for transactions that are made via the mobile channel.

This result was consistent regardless of whether or not the organization had actually deployed mobile applications that were being used for transactions. Perhaps more significantly, authentication ranked as the number-one security challenge for those organizations that have actually rolled out such applications, and therefore have experience with these issues – and it exceeded 40 percent (remaining the top concern) for those organizations that have rolled out a number (four or more) of these applications.

Moreover, the survey showed that while companies that had not yet rolled out transactionally based mobile applications viewed the protection/encryption of data as the greatest concern (close to 60 percent of those surveyed rated it so); the view of those with experience once they had rolled out these applications was that authentication was much more of a challenge. Again, this view increased as more applications were deployed.

Addressing the Authentication Challenge

Strong authentication protects both the company and the customer. From the company’s perspective, strong authentication means the user cannot refute charges or rescind an order claiming the organization didn’t carry out the transactions. From a user’s perspective, strong authentication prevents someone else from accessing his or her account and conducting unapproved transactions.

Authenticating users is essential to a successful mobile transaction application. Survey respondents indicated that they use a variety of security methodologies, including username and password, digital certificates, one-time password tokens, question and answer, and SMS soft tokens.

However, far and away, the most common authentication method used by survey respondents’ companies (and the rest of the world) is username and password.

Unfortunately, most users pick simple passwords. How simple? A 2010 eWEEK Security Watch article¹ discussing an analysis of 32 million passwords compromised in a service provider breach noted that the three most common passwords were 123456, 12345, and 123456789. Other common passwords included “Password” and “iloveyou.” In fact, about 50 percent of the accounts used names, dictionary words, or trivial passwords (e.g. consecutive numbers).

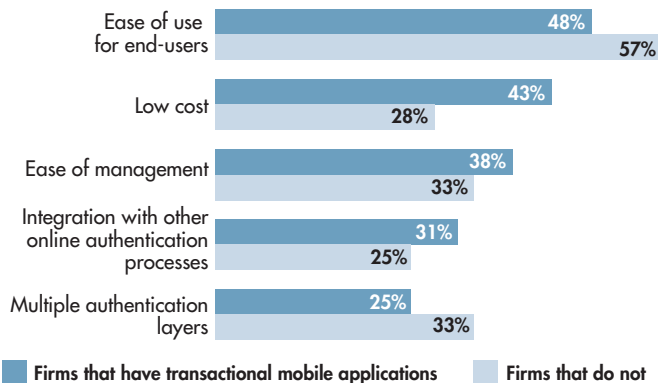
1. “Rockyou Breach Analysis Reveals Insecure Passwords,” eWEEK Security Watch, January 21, 2010

This reinforced the findings of an earlier study on password weakness conducted by the University of Wisconsin-Madison and IT University in Copenhagen. Reporting on that study, a 2009 *eWEEK Security Watch* article² noted that “only four percent of 836 people surveyed obeyed best practices for passwords.”

The take-away from these and other studies is that users and their passwords are a major security weakness. The problem with such passwords is that they are easy to guess using a minimal amount of brute force.

While there are various means of authenticating users, the paramount consideration in the mobile space is its ease of use for end-users. In fact, regardless of whether the organization surveyed had already deployed transactions via mobile applications, the most critical consideration among firms implementing or upgrading their authentication capabilities was “ease of use for end-users.” Close to 60 percent of those who have yet to roll out such applications, and close to 50 percent of those with experience, considered this the prime consideration. Low cost and ease of management/maintenance were also compounding considerations, after addressing the ease-of-use concern.

Most Critical Considerations for a Firm When Implementing/Upgrading Authentication Capabilities



Capitalizing on the Opportunity for Transactionally Based Mobile Applications

Ultimately, to capitalize on their plans to move more of the transactions currently offered in the traditional online channel to the mobile space, organizations need to solve some of the inherent security issues and address these perceptions among their end-users.

An important first step in this direction may be to capitalize on using the mobile device itself to enhance security for traditional online transactions.

As noted, 20 percent of the more experienced firms surveyed recognized the potential to use the device in this way. This practice could expand the transactions currently offered online and enhance customer satisfaction.

While solving some of the security issues is within an organization’s control, experience demonstrates that there remain key challenges that must be addressed – particularly with regard to authentication. Here, organizations must implement an authentication strategy that is considerably stronger than the ubiquitous User Name/Password approach.

While the solution should address considerations regarding cost and management, the primary goal must be to implement an approach that is easy for end-users.

Proven Expertise

Organizations that currently provide their online users with transactionally-based services need to extend these services to the mobile channel if they are going to protect and grow their user base. But to succeed, they must start to solve the security dilemma – and the most important challenge to be faced is solving issues around authentication. An important first step is to enable current web applications to be accessed from the mobile device, with an appropriate authentication method supported by the web application. From there, authentication will evolve on mobile applications themselves.

Underlying the authentication challenge is the need for companies to select a versatile authentication platform that supports a broad range of authenticators, so different types of authenticators can be applied to different types of users depending upon the risk associated with the transactions being done. Organizations also need to ensure that the underlying authentication platform can be expanded to support with new authenticators as the market evolves. This ensures that mobile devices can leverage the same underlying platform as transactional services evolve, from the web to the mobile device.

More than 4,000 organizations in 60 countries across the globe leverage Entrust’s world-class solutions, which include SSL, strong authentication, fraud detection, digital certificates, public key infrastructure (PKI), ePassport security, email security, and more.

For more information, go to:
www.entrust.com

2. “Password Strength Needs a Boost,” *eWEEK Security Watch*, October 16, 2009