

P E R S P E C T I V E

## What the Future of Online Banking Authentication Could Be



YOUR INNOVATION PARTNER

## Banking on Internet and mobile is gaining popularity

The Pew Internet & American Life Project Tracking survey of December 2010 said that nearly 60% of all Americans who used the Internet did some banking over it. In the United Kingdom, the number of bank accounts registered for Internet banking grew sharply from 28 million in 2006 to 45 million in 2010. With over 100 million, a Chinese bank has the largest number of Internet banking users in the world.

Cut to mobile banking. A research firm estimated that about 110 million people worldwide used mobile banking and related services in 2010. It also indicated that the geographies of Asia Pacific, Middle East and Africa would be the most important markets for financial services using the mobile device. Another one forecasts a stupendous 660% growth in mobile banking and payment services between 2009 and 2014.

A number of factors, including lower cost of connectivity, greater Internet and mobile Internet penetration, affordability of devices and the arrival of the smartphone have gone into popularizing online (Internet and mobile) banking around the world.

### However, security threats continue to loom

While these figures are impressive, these could have been higher, had it not been for the security threats surrounding online banking such as phishing, pharming, hacking, keystroke logging, Man-in-the-middle, Trojan horses and several other modes of attack that discourage adoption. The fact remains that despite advancement in security technology, fraudsters still manage to breach banks' defenses from time to time. Consider these numbers: every month, around 18,000 phishing attacks take place around the world; 3% of Internet users from the EU27 group of countries lost money to online fraud last year; and there are at least 2,500 varieties of e-banking malware. Nearly 80% of U.S. banks think that malware on their customers' PC is a top security risk. Indeed this seems justified because U.S. consumers lost over US\$ 2 billion and 1.3 million PCs to malware in 2010.

A compilation of the security threats to mobile and online banking in 2011 ranked malware distribution through social networks, attacks targeted at specific organizations and theft of financial information using malware, at the top.

While fear of fraud has kept a number of customers all over the world from using Internet or mobile banking, at the same time, it has made banking institutions more cautious with their security policies. While there are many threats as described above, a very strong authentication mechanism for customers and transactions will address most fraud related issues. In addition to employing authentication techniques some banks also resort to other measures such as limiting the number of online banking operations that a customer can perform each day, capping the value of individual transactions, or applying additional layers of user authentication in the case of high value or exceptional transactions. On the face of it, banks apply such restrictions to protect their customers. There is also an element of self-interest in it as the banks would like to limit their own risk as well in the event of a transaction being initiated by someone who is not authorized to do so.

### The current state of online banking authentication

Having mentioned earlier that authentication of customers and transactions forms the foundation in preventing of online banking fraud; let us look at the current state of online banking authentication models. At present, authentication of online banking users is done using any or a combination of the following methods:

**User Id and password:** This is the most popular and common method, which involves asking users to enter their User Id and password. As additional security, users may be required to ensure that their passwords are strong, change them routinely after a fixed number of days, or may be assigned a different one for transaction authorization.

**Two-factor authentication:** This method verifies users' identity based on something that they know (user name and password) and something else that they have. For example, a bank might provide a token (physical or virtual) to customers,

who, besides entering their password, must enter a random number generated by the token to authenticate themselves each time they conduct a transaction – like a payment, for example. Alternatively, the bank might send a One Time Password (OTP) to the customers' registered mobile device each time they initiate that transaction. In addition, the bank might subject customers to further scrutiny in case they are performing high value transactions or indulging in any activity that arouses suspicion. Some banks also verify the IP address of the device using which a customer performs a transaction, and should that change, resort to further querying and other forms of additional authentication.

The extent of authentication varies across banks, and depends on its security infrastructure as well as its risk tolerance guided by its risk policies. No doubt, two-factor authentication is more effective at preventing impersonation, but, as the recent breach of RSA's tokens showed, it is not 100% foolproof – in fact, a study of banking fraud-related challenges in Latin America showed that almost a third of token users didn't quite trust them. This is the reason why banks take the additional precaution of restricting transactions in spite of implementing such security arrangements. That apart, tools of two-factor authentication have other limitations—tokens are expensive to produce, distribute and administer, and OTPs sent via SMS could take time to reach.

### Alternate models of authentication

The recent advancements in emerging technologies could enable new modes of more secure authentication without impacting customer experience. These advancements leverage the inherent capabilities of smartphones to introduce a third factor of identity verification. In three-factor authentication, in addition to furnishing their regular password and an OTP that appears on their token or mobile phone, users will be asked to present something that they possess, which would irrefutably prove their identity. This third factor could be captured using either an application that is installed on the customers' smartphones or an inbuilt feature or capability of the device.

Some examples of the third factor are fingerprint, retinal image and voice. Assume for a moment that a customer is trying to transfer a very large sum of money via mobile banking. In the new model of authentication, after the customer submits his two passwords, an application that is loaded on his mobile will prompt him to provide a third factor, say his fingerprint. The customer places his finger on the smartphone screen, following which the application scans the impression and transmits it to the bank, where it is matched against the fingerprint image in their records.

There are other possibilities of biometric authentication as well, such as capturing words spoken by the customer via his phone and matching them against a previously authenticated sample of voice that exists in the bank's records, or asking him to take a photograph or retinal scan with his smartphone's camera and send it to the bank for approval and authorization.

It is also possible for banks to conduct three-factor authentication of customers who don't own a smartphone, by providing them a device, which can be plugged into their devices which is capable of capturing and transmitting the biometric information.

### Key success factors for adoption of newer models of authentication

Currently, the new models of online authentication are in various stages of evolution, and are yet to be commercialized. Once their technology is perfected, these methods can quickly become mainstream security procedure. The following factors play a critical role in creating a favorable environment for the new authentication models to thrive and grow as mainstream models :

**Infrastructure:** Capture and verification of fingerprint, voice or any other biometric information requires special infrastructure to be set up and integrated. On the capture and verification, support is available from both Government and external agencies, which can capture and store customers' biometric samples as well as provide applications to help the banks verify the information.

**Advancements in storage technology:** Over the years, data storage technology has progressed leaps and bounds that the cost of storage has drastically reduced; the cost per GB of data in 2010 was 1/10th of that in 2000. This combined with increased efficiencies in algorithms of data storage of information such as biometrics has helped banks to attain a position where they could leverage economies of scale with respect to data storage in order to keep the costs of maintaining massive volumes of biometric information manageable. Emergence of the “Cloud” will only accelerate the ability of banks to adopt this trend faster without having to worry about scalability or performance or security of such data.

**Device proliferation:** The adoption of the new authentication methods is directly linked to smartphone penetration. For this reason, these techniques would have been unworkable a few years ago; however, with smartphone usage expected to cross 1.7 billion by 2014, and annual sales growing in the region of 75 to 80 percent, the stage is set to welcome sophisticated forms of authentication in the next 3 to 5 years.

**Business case:** Analysts predict that the spending by banks on anti-fraud solutions will grow at about 30% over the next few years. This is clearly indicative of the industry’s concern about the growing sophistication of fraud techniques, which continue to breach security systems, even as they’ve become stronger. While this is a clear trigger for the adoption of better authentication solutions – such as those built on three factors – banks may not invest in them unless they find that the investment more than pays for itself by way of reduction in fraud.

That being said, factors such as technology advancement, reduction in data storage cost, and the availability of a support ecosystem of external partners are favourable to bringing down the cost of implementation, and will thereby strengthen the business case for adoption of the new security models.

**Regulations:** In many countries, two-factor authentication is already mandatory for performing online financial transactions, and it is quite

possible that this will progress to three factors in future, thus giving the necessary impetus to newer methods.

While the above factors are not directly led by consumer behavior, higher customer adoption of online banking could also force banks to look into sophisticated models of authentication. Many banks across the world are now offering more than just banking transactions on their online banking portals, extending the scope of services to wealth management, transaction behavior-led product sales, virtual banking, customer networking etc. If these strategies start to pay dividends then they could also result in higher adoption of online banking, thus forcing banks to adopt the new models of authentication.

### **This is an ongoing journey**

Signs are ripe that sooner or later, the above mentioned factors will converge to a tipping point when the current methods of authentication will make way for more sophisticated ones.

However, this is not the end of the road. While multi-factor authentication looks like a foolproof solution under current circumstances, it is also true that even this will not stop an attacker forever, but merely slow him/her down. The implementation of security technology is neither a one-time effort, nor a guarantee of lifetime protection. What looks like a cutting-edge solution today will be standard fare tomorrow and out of date a few years thereafter. But for now, the future of online banking authentication appears headed in the direction discussed in this paper.

### **Reference:**

1. Financial Institutions Must Address Security Concerns in Mobile Banking and Payments, April 21, 2011.  
[www.mobilecommercedaily.com/2011/04/21/financial-institutions-must-address-security-concerns-in-mobile-banking-and-payments](http://www.mobilecommercedaily.com/2011/04/21/financial-institutions-must-address-security-concerns-in-mobile-banking-and-payments)
2. Smartphone Growth Explodes, Dumb Phones Not So Much, Feb 7, 2011.  
[technolog.msnbc.msn.com/\\_news/2011/02/07/6005519-smart-phone-growth-explodes-dumb-phones-not-so-much](http://technolog.msnbc.msn.com/_news/2011/02/07/6005519-smart-phone-growth-explodes-dumb-phones-not-so-much)

3. Bank Tech Spending to Hit \$132B in 2015, Analysts Say, Jan 12, 2011.  
[www.computerworld.com/s/article/9204760/Bank\\_tech\\_spending\\_to\\_hit\\_132B\\_in\\_2015\\_analysts\\_say](http://www.computerworld.com/s/article/9204760/Bank_tech_spending_to_hit_132B_in_2015_analysts_say)
4. People Bank Online, but Prefer Branches for Service, Oct 4, 2010.  
[thefinancialbrand.com/13695/consumer-banking-preferences-in-canada-united-states/](http://thefinancialbrand.com/13695/consumer-banking-preferences-in-canada-united-states/)
5. Global Mobile Statistics.  
[mobithinking.com/mobile-marketing-tools/latest-mobile-stats](http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats)
6. E-banking Security Stats.  
[www.ebankingsecurity.net/stats/](http://www.ebankingsecurity.net/stats/)
7. Pew Internet & American Life Project, Trend Data.

[www.pewinternet.org/Static-Pages/Trend-Data/Online-Activites-Total.aspx](http://www.pewinternet.org/Static-Pages/Trend-Data/Online-Activites-Total.aspx)

8. AhnLab Highlights Top 10 Security Threats in the First Half, 2011 July 28, 2011.  
[www.businesswire.com/news/home/20110728005912/en/AhnLab-Highlights-Top-10-Security-Threats-2011](http://www.businesswire.com/news/home/20110728005912/en/AhnLab-Highlights-Top-10-Security-Threats-2011)
9. Smartphone Usage Set to Rocket to 1.7 Billion by 2014, 27 April 2010.  
[www.independent.co.uk/news/business/news/smartphone-usage-set-to-rocket-to-17-billion-by-2014-1955258.html](http://www.independent.co.uk/news/business/news/smartphone-usage-set-to-rocket-to-17-billion-by-2014-1955258.html)

**Author**

**T C Dinesh**

Senior Principal  
Infosys Limited



YOUR INNOVATION PARTNER

PERSPECTIVE

Universal Banking Solution | System Integration | Consulting | Business Process Outsourcing

#### Infosys Limited

Plot No. 44, Electronics City, Hosur Road, Bangalore - 560100. India  
Tel.: + 91 80 28520261, Fax: + 91 80 28521747, e-mail: [finacleweb@infosys.com](mailto:finacleweb@infosys.com)  
[www.infosys.com/finacle](http://www.infosys.com/finacle)

Join us on Twitter, LinkedIn and Finacle Whiteboard at [www.infosys.com/finacle/networking.asp](http://www.infosys.com/finacle/networking.asp)

\*COPYRIGHT NOTICE: Copyright ©2011 Infosys Limited, Bangalore, India. ALL RIGHTS RESERVED.  
Finacle logo is a registered trademark of Infosys and Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.