A Common Login System?

Sherman Tan

09 Apr 2010

Common security system by 2015

Last month as part of the Budget 2010 update, Lui Tuck Yew, Singapore Acting Minister for Information, Communications and the Arts informed that a new online security system will be in place by 2015 that will allow consumers to access the websites of banks, government agencies and health care providers using the same security device. One of the benefits of this common system is to address the core issues of banking customers having to use different hardware devices (tokens) provided by banks to access their online financial services. Secondly, it also allows the government to strengthen Singapore's internet infrastructure and the comprehensive host of e-government services against the increasingly sophisticated cyber threats.

Some history

Prior to 2006 before banks here are required to provide an additional layer of dynamic authentication in addition to the mandatory login with static user ID and password, there were discussions as far back as 2000/2001 when there was a call by the Ministry of Finance for a common login system for banks and e-government services. However, as there were significant differences in which how different banks and government agencies implement web security for the types of services that they offered; eg a breach on the leakage of CPF information on the web while important does not involve physical lost of cash by a customer should an unauthorized online transfer be made; hence the idea of a common login system was temporarily shelved.

However, riding on the wave of web services, NTUC Income launched the "Big Trumpet" in Oct 2002 in collaboration with Microsoft. Touted as the single portal for the community, "Big Trumpet" was to provide a wide range of services including job-matching, secured depository for sensitive electronic documents and bill payment services from various banks. An aggregated portal of services with single sign-on access may seem an attractive business proposal on paper but this ambitious plan was slow to catch on the public interest as it became clear to business analysts and marketers that while consumers want convenience, they also want choice and alternative means of doing things. That's one of the reasons why from a theoretical perspective, a "all-in-one" ATM/credit/debit/loyalty point/identity/security access card will be a powerful card that will be treasured by all customers but in reality; there is lacking in demand for such a card as the misplacement/theft of such a powerful card can potentially lead to very serious consequences.

So much for the "benefits" and "attractiveness" of a common online portal and "all-in-one" card so let's move on to the single-sign-on solution that is supposed to bring convenience and benefits to users of internet services as well.

Windows Live ID that we use today to login to a suite of Microsoft website services such as Hotmail, MSN, MSNBC, Xbox Live, etc originated from Microsoft Passport since 1999. With the proliferation of email hosting services, commercial and financial services websites that require some form of user authentication, internet users often have difficulties remembering the different login credentials for these websites. However, the introduction of Microsoft Passport was perceived as a threat by competitors who fear that Microsoft will gain dominance over the internet once it is able to manage and store the login credentials of millions of internet users. Hence, along came Liberty Alliance formed by Microsoft competitors that announced the First Liberty Alliance Specifications for Open, Federated Network Identity in Jul 2002.

Since then, both groups have taken on a separate path in developing their common security authentication systems and frameworks. Very briefly, Microsoft adopted OpenID in Aug 2008 and became an OpenID provider in Oct that year. Meanwhile, the Liberty Alliance introduced the Identity Assurance Framework (IAF) in 2008 and this piece of work was pursued by the Kantara Initiative Identity Assurance Work Group (IAWG) in 2009 to further foster adoption of identity trust services.

Various concerns

Microsoft Passport was plagued by lots of criticisms after it was introduced; the main criticisms were centered on privacy issues of internet users, earlier security flaws in the design of the single-sign-on system and the concern that the central storage of huge amount of customers login information will make the Microsoft databases like "honey-pots" for hackers. Moreover, over the years, initial key supporters of the Microsoft Passport/Windows Live ID broke-off; some big names include eBay and Monster.com. Just last year, Expedia; an online travel portal also announced that it no longer support Microsoft Passport and Windows Live ID for their web portals.

Microsoft's adoption of OpenID and becoming a provider of OpenID is probably partly to ally concerns that Microsoft could dominate the access means to the wide range of online services on the internet and other distributed networks.

OpenID begun in 2005 and was based on an open, decentralized standard to authenticate users. Basically, OpenID provides a user with a single login method at a trusted service provider to automatically access services of other websites. For instance, a user who has already been digitally authenticated by service provider 'A' will not need to create a new account or re-sign-in using different sign-in requirements at service provider 'B" website.

To access website of service provider 'B', the user needs to provide his OpenID to 'B' instead of creating a new account with 'B' or re-entering his credentials registered with 'A' again. This open and decentralized authentication protocol; give users the benefits of using a single OpenID to access multiple websites that adopt OpenID standard. Moreover, from a conceptual perspective, it also minimizes the possibility of a single party gaining dominance over the others in the area of authentication control as it is left to the users to decide which party they want to register their OpenID with. To date, besides Microsoft, corporate members of the OpenID foundation include Yahoo, Google, MySpace, PayPal, IBM, Sun Microsystems, Facebook, VeriSign, etc.

While OpenID is gaining recognition and endorsement by many established organisations, some observers have suggested that OpenID could be vulnerable to phishing attacks involving a malicious relying party using a bogus identity provider authentication page to ask a user to input his credentials. Once such information is secured, the malicious party can then masquerade as the user to login to other websites using his OpenID. To combat such attacks, it is now mandatory for OpenID providers; eg Microsoft to require the user to authenticate with the former before he authenticates with the relying party. Despite this measure (as part of the OpenID Foundation approved version 1.0 of the Provider Authentication Policy Extension) spelt out in end-2008, concern over "man-in-middle" phishing attacks remain.

Looking ahead

While it is commendable that Singapore is committed to establish a common security system for banking, e-government and health care services, there still exist many key issues to be addressed. First and foremost, the planners must decide whether the long term plan is to provide a common login platform for only local online services and the standard to be adopted?

An example is that it is probably not too far in the distant future where health care services could be offered by countries beyond Malaysia. If the intention is to help users better manage their online security including off-shore online and other social/community-based services, a globally established standard will have to be factored into the design of the system. In which case, careful evaluation of the various types of standards available needs to be made.

Secondly, past issues surrounding the need for different security levels still exist in various forms. For instance, hackers will not find meaningful monetary gain from impersonating users for e-government services other than creating mischief by fraudulently submitting say HDB flat application. However, some e-government services such as transfer of CPF funds between different types of CPF accounts could result in more severe consequences including the need to re-compute losses in interest, denial of medical services due to insufficient funds in the Medisave account and more. In the case of health care services, a compromise in the access or corruption of patient's medical depository could potentially lead to inability to retrieve an important medical report during time sensitive condition.

In addition, as mentioned earlier in the article, financial service providers place different security requirements pertaining to securing confidential information vis-à-vis authorization to execute a financial transaction. For the latter, non-repudiation is essential in the event the transaction is disputed by the customer. Adding to the complexity of the equation, regional foreign banks that offer financial services here may have some level of challenges to adapt to our local common security system which could be contrary in requirements to its own regional security implementation strategy.

Helping online users better manage their security is very important and the approach must take into considerations the various needs and challenges; some of which are highlighted above. The task force assigned to execute this has 5 years to do so.

The writer is the Principal Consultant & Director at Innovar Pte Ltd (www.innovar.com.sg). He can be contacted at office@innovar.com.sg.