Security and Social (Media) Banking

Sherman Tan, PMP

30 Oct 2014

Cyberthreats: The Endless Defence

Last month, the Google security team reported a security flaw, the POODLE attack (Padding Oracle On Downgraded Legacy Encryption) which is a "man-in-the-middle" exploit that takes advantage of any website that support SSL 3.0 (Secured Sockets Layer). Two weeks later, BASH; a collection of security bugs that are associated with the widely used UNIX Bash Shells was reported.

These critical flaws comes hot on the heels of Heartbleed that was reported in Apr and by 20 May 2014, 1.5% of the 800,000 most popular TLS-enabled websites[1] were still vulnerable to Heartbleed. News reported on 14 Oct 2014 that nearly 7M Dropbox user accounts were compromised[2] added on a greater sense of insecurity and helplessness for the masses who are so accustomed to using the web and social media applications.

When internet banking became main-stream in early 2000, the main connectivity to banking systems from non-bank owned devices was predominantly via the customer's desktop or PC. Mobile broadband, high speed connectivity and wide spread adoption of smart phones and other connection-based devices significantly changes the goal-poles and rules of the game for security and IT professionals.

So it came as no surprise when Deloitte research[3] last year found that the top three reasons for the rapidly evolving threat landscape were:

- Growing number and type of third parties: 78%
- Increased usage of mobile devices: 74%
- Lack of sufficient employee awareness: 70%

To make matter worst, owners of recently compromised services such as Dropbox, Snapchat and iCloud have pushed the blame to users and third-party application providers instead of scrutinizing the types of third-party applications that can access their services.

Accessibility, Convenience, Productivity versus Safety and Security

Until the arrival of the first Ford T model in late Sep 1908, cars were often viewed as extreme luxury for the masses. But by 1927 – 19 years later, 15M[4] Ford T model cars rolled off the Ford factory. The availability of affordable cars has since changed the lifestyles of many millions in the world.

Some 106 years later, notwithstanding advances in technologies and new materials available, recall rates of the modern cars remained high.

In a Forbes article this year[5], the top 5 automakers with the highest recall rates since 1985 were: General Motors (99.3M), Ford Motors (97.0M), Chrysler Group (63.2M), Toyota Motor Corp (38.6M) and American Honda Motor Co (31.1M). Other headline catching stories includes the recall of 6.5M Bridgestone tyres (2000) that lead to 600 injuries and 271 death, 8.5M Toyota cars recalled in 2009 due to power steering failure resulting in 16 death, 243 injuries and 2,000 accidents and General Motors recalling 1.5M cars (2010) due to engine fire and 14 accidents[6].

While the revolution (of the affordable car) has brought about a host of direct and indirect benefits to the families and global economics, the World Health Organisation (WHO) reported 1.24M traffic accident death in 2010[7] alone making it the 8th leading causes of death globally similar to some communicable disease such as malaria. However, there is a silver lining as the number of road fatalities has plateaued since 2007 against a 15% increase in the number of registered motorized vehicles over the same period. Amongst several contributing factors, the WHO attributed the five pillars that guide national road safety plans and activities in many traffic accident prone countries:

Source: World Health Organisation "Global Status Report on Road Safety 2013 – Supporting a Decade of Action"

The United Nation of Assembly has endorsed the WHO's action plan in 2010 with a goal to save 5 million lives globally from 2011 to 2020 through the implementation of the 5 core pillars and the reduction of 5 key risk factors namely, speed, drink-driving, helmets, seat-belts and child restraints commonly associated with traffic fatalities.

The numerous actors involved, e.g. governments, industry associations, road safety councils, highway engineers, automobile manufacturers, insurers, consumers, etc understand the benefits of the safe use of motorised vehicles and the need to work together to make the entire ecosystem a much safer one for all that are involved in its partake. In some countries, more than a nudge is required from national or international governance bodies to push through roadblocks in certain areas.

So what has banks got to do with road safety?

Financial Services and the Social Media Environment

The drivers for banks to transform digitally and embrace the social media have been discussed in earlier articles by this author[8].

At the macro level, banks are not unlike automobile manufacturers – producing and delivering products and services to their customers. Not only must these products and services be easily accessible, affordable, add-value, easy to use, befitting of the lifestyles and needs of the customers but are also safe and secure. Again, not unlike automobile manufacturers, the environment involves many inter-dependent parties to ensure that these financial products and services can be delivered and enjoyed in a safe and beneficial manner by bank customers.

This is not a new concept as some writers in the past have envisaged that the internet as akin to the public highway. Initially, quite unsafe due to fewer road signs, lack of street lighting, unclear traffic rules, and of course, amateur "drivers" without knowledge of internet security venturing into phishing and unsecured websites. This situation has improved somewhat over the years with more better educated and discerning users, wider varieties of internet security software, more frequent and timely updates on security flaws and breaches but the wide spread adoption of smart phones, connected portable devices and social media applications have however, changed the entire thread landscape.

Nonetheless, the 5 pillars adopted by the WHO to improve road safety in this author's view could still be adapted as a guide for banks when developing and offering financial services for their social media customers.

Just as Asian banks are calling for stronger "Asian voices" in global discussions about industry regulatory reform that will impact Asian economies, banks should likewise actively engage their regulators and participate in regional and national level infocomm security committees to influence and shape the outcome for a safer environment to implement and deliver financial products and services over the internet and social media platforms.

Tabulated below are some potential areas the banking industry could consider in developing a framework to manage the increased threats of cyber-attacks:

Table 1: 5-Pillar for Better Security Management of Social (Media) Banking

Pillar	Core Theme	Possible Considerations
1	Cyber security framework and guidelines	▪ Lobby government bodies and regulators to develop forward looking and market responsive guidelines and legislation to cultivate and promote safe use of social media for the financial industry ▪ Active participation in regional & national level Infocomm security councils and committees to put forth industry specific needs, influence and shape outcome that benefit the financial and other key industries
2	Safer web, mobile, social media, financial, payment infrastructure & applications	▪ Collaborate with national-level infocomm agencies, telcos, cybersecurity agencies, educational institutions, major hardware/software vendors to develop good practices and minimum standards for development, testing and maintenance of social media applications ▪ Consider setting up accreditation centres to facilitate organisations and individual developers/manufacturers who want to send their applications/devices for voluntarily accreditation ▪ Establish a data base where the general public could access to identify those organisations that have adopted the specified industry standards and those who have obtained accreditation ▪ Standardise core criteria to rate buyers and sellers in B2B, B2C and P2P platforms ▪ Set up community based monitoring systems for timely dissemination and alert of irregular activities involving suspicious buyers and sellers
3	Safer web and social based financial products and services	Beyond existing security and risk management policies and practices, banks should evaluate how to adopt full or partial use of social media credentials to facilitate "friction-less" on-boarding of new customers or sign-up of new services by existing customers. Possible considerations could include: ▪ Additional authentication/verification methods such as those use by MOOC providers to authenticate registered users when performing online exam, enhanced voice-based authentication when signing up for new email account, location-based information, etc ▪ Verification of robustness, creditability and security of third-party application service providers ▪ Use of Big Data analytics to analyse, monitor and highlight potential risk adverse activities in real-time or near real-time basis
4	Safer web and social media users	▪ Continued education for web/social media users be conducted on a more regular basis and making these programmes more accessible ▪ Incentive schemes to sign-up more users and this could be in the form of bonus points, reward certificate, user-level recognition akin to different user level in online games ▪ Since a high % of cyberattacks originate from within the organisation, users and bank staff should be trained to identify suspicious co-workers, awareness of social engineering, adopt safe practices when using own devices to access, conduct corporate-based and financial transactions
5	Post incident management and recovery	▪ Many organisations and banks included are reluctant to openly admit that their services or systems have been compromised, this mind set has to shift as timely sharing of security bleaches could help minimise attack of other organisations who could be exposed to similar vulnerabilities ▪ While banking authorities such as the Monetary Authority of Singapore (MAS) has stipulated a set of stringent requirements for banks to inform MAS of security breaches, this is for regulatory reporting and compliance purpose – as an industry, banks could collaborate further as an extension of Pillar 2 to strengthen its industry group against cyberattacks and cybercrimes

More than Road Bumps Ahead

The 5-Pillar framework is not going to be easy to implement by any single financial institution as it requires strong leadership and collaboration from other members that are genuinely interested in working together to create a safer environment to offer social (media) banking. From previous experience, it is evident that regulators across the globe are likely to adopt a wait-and-see attitude resulting in the emergence of a significant number of non-bank payment service providers as well as proliferation of different types of virtual currencies.

Banks themselves are likewise responsible for the current state of affair as many are too focused in protecting their respective interests instead of allocating resources to develop the desired environment for the common good. In a number of national-level, industrial-led projects, individual party's interest often results in project delays and in some cases, risks of project being aborted. The recent warning from the Reserve Bank of Australia[9] and the acknowledgement by the US Clearing House that while it is late in moving into real-time payment, the implementation is "a comprehensive multi-year endeavour requiring coordination among financial institutions of all sizes and their service and technology providers"[10].

The situation however is not a dire one. For instance, members of the Bank Governance Leadership Network have met twice this year to discuss the challenges and opportunities in digitalisation in banking[11]. Although no new legislation has been introduced, the Federal Financial Institutions Examination Council (FFIEC) has released its final guidance to US banks on Social Media in Dec last year[12].

While slow progress is made, opportunities arise for non-banks players to stake their claims especially in the areas of mobile and electronic payments space that are intimately embedded in social media offering. It is of interest to note as far back as a year ago, PayPal and eBay that foresee significant business potentials in electronic and mobile payment in Asia Pacific have put forth their proposal for new sets of governance framework for electronic and mobile payments[13].

Transforming banks into Social (Media) banks would undoubtedly lead to significant re-alignment (and disruptions) in many key aspects of banking practices, governance structures, culture and people mindset, security and risk management amongst others. But such transformation is no longer an option if banks are to stay relevant in the world of social media.

Notes:

[1] *"AVG on Heartbleed: It's dangerous to go alone" 20 May 2014: http://www.theregister.co.uk/2014/05/20/heartbleed_still_prevalent/*

[2] *Business Insiders Singapore 14 Oct 2014: http://www.businessinsider.sg/dropbox-hacked-2014-10/#.VEnv1ZVEj4Z*

[3] *Deloitte: "A wave of digital change - Trends in digital E-nnovation 2013" 8 Oct 2013: http://www2.deloitte.com/global/en/pages/about-deloitte/articles/pl-digital-trends.html*

[4] *Wikipedia: Ford T Model: http://en.wikipedia.org/wiki/Ford_Model_T*

[5] *Forbes "Automakers with the Lowest (And Highest) Recall Rates" 26 Mar 2014: http://www.forbes.com/sites/jimgorzelany/2014/03/26/automakers-with-the-lowest-and-highest-recall-rates/*

[6] *Statistic Brain "Automobile Recall Statistics": http://www.statisticbrain.com/automobile-recall-statistics/*

[7] *World Health Organisation "Global Status Report on Road Safety 2013 – Supporting a Decade of Action": http://www.who.int/violence_injury_prevention/road_safety_status/2013/en/*

[8] *Sherman Tan, "Digital Transformation in Banking is No Longer an Option", 25 Aug 2014: http://www.innovar.com.sg/more.htm#Digital_Transformation_in_Banking_is_No_Longer_an_Option and "The Everyday Bank", 25 Jun 2014: http://www.innovar.com.sg/Archives/Everyday%20Banking_25Jun2014.pdf*

[9] *FineXtra, "RBA warns Australian banks not to backtrack on payments modernisation", 24 Oct 2014: http://www.finextra.com/news/fullstory.aspx?newsitemid=26620*

[10] *Digital Transactions, "Pressure Builds for Faster Payments As The Clearing House Plans for Real-Time Settlement", 23 Oct 2014, http://www.digitaltransactions.net/news/story/Pressure-Builds-for-Faster-Payments-As-The-Clearing-House-Plans-for-Real-Time-Settlement*

[11] *E&Y: Leading the digital transformation of banking_06Aug2014: http://www.ey.com/Publication/vwLUAssets/ey-bqln-viewpoints-leading-the-digital-transformation-of-banking-6-august/$FILE/ey-bqln-viewpoints-leading-the-digital-transformation-of-banking-6-august.pdf*

[12] *Federal Financial Institution Examination Council, Final Guidance on Social Media, 11 Dec 2013: https://www.ffiec.gov/press/pr121113.htm*

[13] *PayPal & eBay, "Payments Regulation Framework for Asia Pacific: A Model for Innovation and Growth", Oct 2013: http://www.ebaymainstreet.com/sites/default/files/PayPal-Payment-Regulations-Booklet-APAC.pdf*

Sherman Tan, PMP is the Principal Consultant & Director at Innovar Pte Ltd (www.innovar.com.sg). He can be contacted at enquiry@innovar.com.sg.