A Fundamental Challenge for the Banking Industry: Better Authentication in Electronic Infrastructure

Karl Frederick Rauscher and Didier Verstichel

1. Introduction

Banks and other financial services firms have invested heavily in technology during the past fifty years to measure, monitor and control risk, and also provide convenient and efficient delivery of banking services between institutions and to their customers. With respect to the latter, the industry has come a long way since the introduction of the first automated teller machine in 1967 by Barclays Bank in London. Recent years have seen the pace of change accelerate rapidly as technological improvements have greatly reduced the cost and increased the efficiency and functionality of mobile service delivery. This has lead to new risks and new competitive pressures. Some non-bank competitors, who are offering banking and financial services, are unregulated or lightly regulated. Transactional security is a constant challenge due to the variety and volume of threats.

Nearly two years ago, The SEACEN Centre held a Cyber Security Summit with regulators and technology experts to discuss the implications of these industry trends and how to control risks to individual institutions as well as financial stability risks.[1] One of the main conclusions was that bank regulators need to emphasize the engagement of institutions' senior executive management and boards of directors in controlling these risks. Technology risk is a strategic business risk that needs proper oversight at the highest levels of a firm. A fundamental aspect of that risk concerns the authentication of individuals – whether within banking institutions, or as end users.

2. Understanding a Core Challenge of the New Paradigm: Authentication

For some time now, the world of banking has become essentially electronic. Banks have traditionally focused on safeguarding physical assets as the primary means of protecting the value entrusted to them. In this new paradigm, where we are dealing primarily with electronic data and transaction, protecting physical assets has been overtaken with a new priority.[2] Now, the primary concern for banks protecting the value entrusted to them is about managing identities, i.e., who is it that you are dealing with?[3] In the modern world, the actual possibilities are an authorized person, an unauthorized person, or not even a person, i.e., a machine.

Banking, like the rest of society, has been transformed by the benefits of pervasive connectivity, and as a trade-off, now also shares the cyber security risks; risks that are now here to stay. These risks have been recognized by the industry as a major operational concern for well over a decade.

"The Bank for International Settlements' Basel Committee on Banking Supervision introduced operational risk as an element of the first of its "Three Pillars" of sound banking practice. The Basel II Accord defines *operational risk* as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." In modern banking, "processes" are largely performed via electronic means. Likewise, "people" perform their various functions in a banking environment via electronic means. Even the banking "systems" are implemented by electronic means. The inescapable conclusion is that due diligence in cyber security is central to operational risk management."[3]

The challenge of cyber security is everywhere; it is faced throughout the entire banking system, from regulators to all banks, even the smallest retail banks. The weakest link for any of these banks' electronic systems is the entry point, when access is initially granted. One of the conventional practices has been to manage an individual's access via a unique username and password. With the proliferation of such interfaces in their lives, individuals are required to manage a large number of passwords, which they usually write down, or otherwise record, somewhere, bringing into question the whole security of the process. If not required to be more rigorous in their design, individuals tend toward quite predictable passwords, as surveys of the most common choices reveal: "123456", "password", "12345678", and "qwerty".[4]

Another conventional approach for authentication is the required use of a second factor such as a secure token. However the inconvenience of carrying such additional devices is undesirable to customers. In addition, unlike a biometric factor, such devices can be misused by an unauthorized individual who may obtain knowledge of the assigned user's pin. In the eyes of expert observers, these conventional approaches are falling short in keeping up with the expectations and needs of the emerging environments requiring secure authentication.

In seeking new solutions, it may be instructive to consider the forces behind the use of electronic systems that are so compelling: *convenience, speed and cost reduction*. These forces are each relevant to consumers, bank employees and bank managers across the banking industry. Fighting these trends is difficult, if not impossible. Thus, the ideal solution space is to offer effective countermeasures to both (a) improve cyber security and also (b) be convenient, fast and cost effective.

3. Countermeasures with Promise

Fortunately, there is a solution space where these requirements can be met. That is, there are approaches that align with the forces just described, and that are also more effective in providing secure authentication. The Fast Identity Online (FIDO) Alliance is an example of a strong move underway to make online

authentication *more effective*, while also keeping in mind the need to be convenient, fast and cost effective. The mission includes "developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users; operating industry programs to help ensure successful worldwide adoption of the specifications; and submitting mature technical specification(s) to recognized standards development organization(s) for formal standardization."[5] The initiative is an international, non-profit organization whose membership includes Alibaba, American Express, Bank of America, BC Card, Google, ING, Mastercard, PayPal, Visa and WoSign. The progress of this initiative provides ample evidence that an international movement is underway to transform the way authentication is performed.

Many new approaches to improve authentication make use of emerging biometric technologies, including those that exploit the uniqueness of an individual's fingerprint, iris or voice. Other technologies include user habits like body movements, typing speed and patterns that include such aspects as logistics, e.g., location where a function is typically performed by an individual. However, not all technologies and implementations are the same. Considerations going forward will include (i) privacy – protecting the personal biological and other behavior information, (ii) spoof resistance – preventing false acceptance of something fake, (iii) adoption – where there are two aspects: namely, consumer and industry.

In recent years, the use of biometric sensors in smart phones demonstrates a critical mass of public acceptance of the technology. The touch sensors on phones are being used by consumers to conduct a wide range of financial transactions with their banks.

4. Next Steps for the Banking Industry

As institutions take initiatives to improve authentication in the coming years, the practical implementation of new technologies, such as biometrics, faces several hurdles. On the consumer side, there is a huge base of personal card readers and security tokens already deployed that provide two-factor authentication. Biometrics alternatives need to offer improved efficiency and effectiveness. Another challenge for new technologies is the method of enrolling users. The effectiveness and efficiency of such processes must also be at least comparable to existing benchmarks, if not improved.

With respect to bank's back office environments, there is massive legacy infrastructure systems and workstations and, at present, some institutions have committed limited financial resources to invest in new technology. The reality of the situation is that the conventional user identification and password technologies are well entrenched and a widespread change of new authentication technologies will require re-prioritizing development agendas.

It should be kept in mind that technologies develop fast in the Internet age, and therefore, it is prudent for regulators to lend a soft hand when trying to guide the industry. The industry initiatives cited above are evidence of existing, tangible results being produced that are benefitting the industry.

5. Conclusion

In summary, one of the critical cyber security focal points for banks in the coming years should be on improving the authentication of the individuals throughout the entire banking system. Fortunately, there are solutions being developed that *both* meet the demands of current competitive trends, i.e. *convenience*, *speed*, and *cost effectiveness*, and the demand to be *more effective* than practices currently widely deployed. The challenge for many institutions in implementing new technologies that improve authentication are prioritizing funding for new technologies, maintaining current levels of security and maintaining operability of systems and services during transitions to the new technologies.

Karl Frederick Rauscher is a Commissioner and Managing Director of the Global Information Infrastructure Commission, initially an initiative of the World Bank to address the concern of a digital divide. Rauscher designed and facilitated SEACEN's first Cyber Security Summit held in Kuala Lumpur in 2014. He has facilitated the development of over one thousand expert-based voluntary best practices for the reliability and security of electronic systems that are applicable to the banking and other industries. Mr. Rauscher serves on both governance and advisory boards for commercial and non-profit ventures, and has served as a strategic advisor for the financial services sector on five continents for high consequence concerns. He is an inventor with over 40 patents/pending. His work is featured in numerous publications, including major media.

Didier Verstichel provided leadership to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) for twenty years, (through 2014), serving as Chief Compliance Officer, Chief Risk Officer and Director of Enterprise Security & Architecture. He previously worked as a technologist at MasterCard. He is currently a Risk Management Consultant at BNP Paribas Fortis and the Managing Director at DV Enterprise. His LinkedIn profile is https://be.linkedin.com/in/dverstichel

Both authors serve on the advisory board for Sonavation, which develops advanced biometric sensors using ultrasound technology.

The authors can be contacted at karl.rauscher@gmail.com and didier_verstichel@hotmail.com, respectively.

Endnotes

1. SEACEN Cyber Security Summit 2014, *Demystifying Cyber Risks: Evolving Regulatory Expectations*, www.seacen.org/file/file/2014/CyberSecurity/Pre-Summit%20Press%20Release_19August%202014.pdf

2. The authors acknowledge that information systems also require physical protection.

3. On the consumer interface side, there is a standard practice known as "Know Your Customer" (or KYC). Banks should only allow their "known customers" to access their systems.

4. Rauscher Karl, Frederick, (2014), "The Mindset and Management for Mastering Financial Stability in the Cyber Frontier," *SEACEN Financial Stability Journal*, Volume 2, p. 27, May.

5. www.teamsid.com/worst-passwords-of-2014/

6. https://fidoalliance.org/