Utilization and Challenges of Biometrics in the Financial Sector[1]

Masashi Une
Director
Center for Information Technology Studies,
Institute for Monetary and Economic Studies
Bank of Japan

1. Recent Trend of Biometrics in the Financial Sector

Biometrics is used as a way to authenticate customers at automated teller machines (ATMs) and other services in the financial sector. A survey of financial institutions in Japan in 2015[2][3] conducted by the Center for Financial Industry Information Systems (FISC) revealed that banks and other institutions are starting to introduce biometric methods to authenticate customers at ATMs, branch counter terminals, and safe deposit boxes. In addition to finger vein pattern, palm vein pattern, and facial recognition techniques that have already been deployed, financial institutions are now considering iris scanning as a way to authenticate customers.

A growing number of Japanese financial institutions are shifting to IC cash cards at their ATMs as a way to thwart use of counterfeit magnetic stripe cash cards and prevent fraudulent withdrawals. According to a survey by the Financial Services Agency, by the end of March 2015, 16.4% of all cards issued were IC cash cards with biometric features, and 51.8% of installed ATMs are capable of using those features[4]. Most ATMs employ a finger or palm vein pattern to authenticate customers, but now a few banks are conducting trials of ATM transaction services that rely on fingerprint authentication alone and do not require a card or a Personal Identification Number[5].

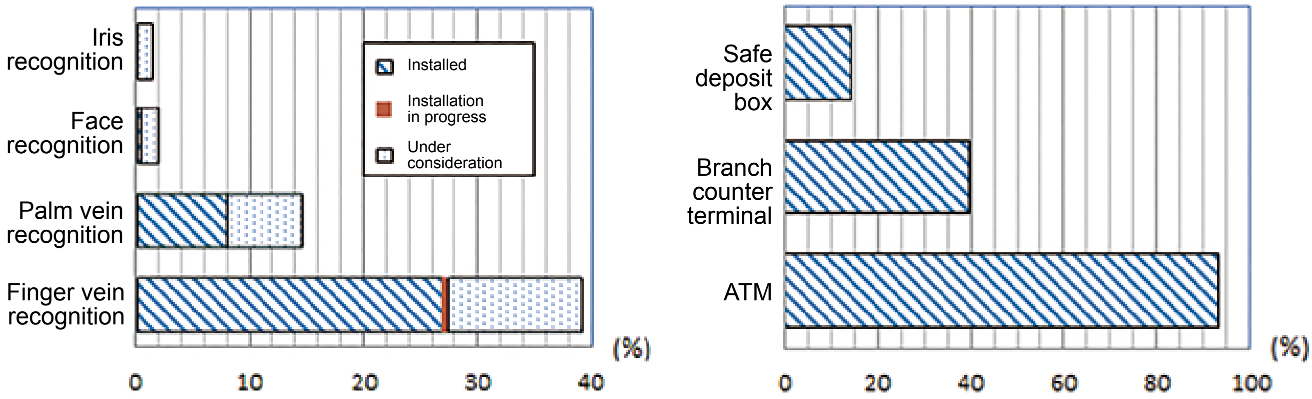
Several foreign financial institutions have adopted biometric authentication for Internet banking. For example, Bank of America introduced fingerprint authentication that enables customers to access services using a fingerprint sensor built into their smartphones in September 2015, and KEB Hana Bank followed with a similar service in February 2016. Both of these services adopted FIDO (Fast IDentity Online), which is a technical specification for implementing biometric authentication over the network[6]. In addition to smartphones, FIDO has also been incorporated in Microsoft Windows 10, and it should see widespread adoption in the future. As the result, biometric authentication may become more prevalent.

From the viewpoint of implementing biometric authentication using smartphones, a palm vein pattern captured with a smartphone's built-in camera has also been proposed for user authentication, and some financial institutions are studying the feasibility of this approach[7].

2. Necessity for Security Evaluation and the Current Situation

The primary purpose of biometric authentication is to detect and defeat malicious recognition attempts by third parties impersonating or spoofing legitimate users. When implementing a system that uses a biometric method to authenticate users (*biometric authentication system*), we have to assume that the system will be subject to a deliberate attack through impersonation or

Figure: Status of biometric deployment in Japanese financial institutions



(A) Authentication schemes implemented by financial institutions

(B) Systems deployed by financial institutions that have introduced biometrics

(Figures based on Center for Japanese Financial Industry Information Systems "2015 Financial Institution Questionnaire Results") spoofing, so it's critically important that we assess and verify in advance the probability that such an attack will succeed (*i.e., attack success probability*). If verification proves inadequate, this raises concern that the system will not be able to detect and defeat the attacks at the expected level.

In the most naïve deliberate attack, the attacker merely presents his own biometric information to impersonate a legitimate user. For this type of attack, assessment indices and methods of measuring the false accept rate (FAR) defining the attack success probability have already been standardized, so systems can be evaluated using these methods.

On the other hand, we must consider the possibility of a more sophisticated attack in which the attacker presents an artifact to the sensor that closely replicates the user's biometric information. Since the year 2000, many academic studies have shown there is a significant probability of artifacts being falsely accepted by several commercial biometric authentication systems[8]. Currently, no standardized security evaluation methods have been established for dealing with artifact attacks, so vendors of biometric authentication systems have been left to come up with their own evaluation procedures, making it virtually impossible to compare evaluation results across different systems.

3. Security Evaluation Research Trends

Recently we have seen a surge of research interest in evaluation of system security in the face of artifact attacks. In May 2015 an academic competition was held to evaluate and compare several finger vein pattern authentication schemes at the International Conference on Biometrics 2015 in Phuket, Thailand. At this competition, a forged artifact—a finger vein pattern printed on paper—was presented to vein pattern sensors; the rate of detecting the fake pattern was then calculated and compared across different schemes.

The Swiss Idiap Research Institute has been developing a finger vein pattern (image data) database. Several studies reported findings based on an artifact created from this database and used to assess some existing finger vein pattern authentication schemes.

Meanwhile, Japan has been pursuing a private-public partnership project[9] to establish a robust security evaluation method for biometric authentication systems. Launched in 2014, the three-year project is being carried out by the Japan Automatic Identification Systems Association, National Institute of Advanced Industrial Science and Technology, and OKI Software Co., Ltd. Goals of the project are to establish security evaluation methods for dealing with deliberate attacks specific to biometrics—including artifact attacks—and to promote international standards supporting third-party evaluation and certification based on standardized evaluation methods. Building on results achieved so far, the project team plans to conduct security evaluation trials using vein patterns on existing authentication systems in fiscal year 2016.

4. International Standardization Trends Relating to Security Evaluation

These recent research findings have led to activities now reflected in international standards. Case in point is the international standard ISO/IEC 30107 series addressing security evaluation methods for dealing with a presentation attack that is now being deliberated in ISO/IEC JTC1/SC37 (Biometrics). The presentation attack involves presentation of some malicious instrument or information with the goal of interfering with the operation of the biometric authentication system to be attacked, and includes artifact attacks.

Security requirements for thwarting presentation attacks are currently under deliberation in ISO/IEC JTC1/SC27 (Security) charged with drafting international standard ISO/IEC 19989. ISO/IEC19989 will be used to evaluate and certify biometric authentication systems in accordance with the Common Criteria (ISO/IEC 15408)[10]. The Common Criteria provides for *testing laboratories* with highly skilled personnel and capabilities that evaluate the security of systems and products, and for *certification bodies* that certify the appropriateness of the evaluation process. Finalization of the ISO/IEC 19989 standard is expected to further bolster evaluation and certification of biometric authentication systems by accredited third parties.

5. Advantages of Use of Standardized Security Evaluation Methods

The establishment of standardized security evaluation methods and use of evaluation and certification results by independent testing and certification bodies will have two major advantages for banks and other financial institutions:

The first advantage is improved security governance. Although the financial sector has been using biometric authentication systems for some time, the security of these systems has not been subject to evaluation by standardized methods. If such methods were available, they could be applied by financial institutions with the cooperation of their vendors to existing systems to determine (a) if countermeasures against presentation attacks are commensurate with the cost and (b) if the countermeasures actually keep security risks below an acceptable level. We would also expect that certification of the adequacy of evaluation by a certification body would appeal to customers and give them a greater confidence in security.

Another advantage of using standardized security evaluation is that this makes it possible to compare the security provided by different biometric authentication systems. Suppose a financial institution wishes to adopt biometric authentication across the board to personal computers, tablets, smartphones, and other devices. When faced with the task of choosing a new biometric authentication system from a host of contenders, naturally one wants to select the system that best satisfies specific security requirements. As it stands now, all we have to go on is the vendor's own assessment of his system's security functionalities, which does not really help in comparing evaluation results among different systems. The ability to refer to evaluation results derived by a standardized procedure not only enables financial institutions to compare the security of different systems, it also permits them to narrow down their search and to quickly identify systems that best meet their particular security requirements.

6. Future Challenges

If financial institutions are to exploit these advantages, it is important for them to consider how they might support research into security evaluation methods and international standardization activities, and how they might utilize evaluation results based on the standardized methods.

In terms of utilizing evaluation results, consider a financial institution faced with the task of choosing a biometric authentication system that will provide a certain level of security against artifact attacks. The process of selection might involve the following steps.

(1) Gather information about all the candidate biometric authentication systems (*e.g.*, systems that have been evaluated and certified by testing laboratories and certification bodies). Be sure to verify from the vendors of the various candidate systems that they are compatible with financial application systems: ATMs, smartphones, tablets, etc.

(2) Obtain documentation used when evaluating and certifying the systems from the vendors such as the Security Target and the evidence of developer testing.

(3) Refer to the documentation obtained in the abovementioned steps, verify that each system fully satisfies the security requirements set by the financial institution: assumed threats (attackers), security policies and functionalities, security evaluation results, and so on. Systems that pass this screening are shortlisted as "candidates providing adequate security against artifact attacks." If more than one system meets this criterion, narrow the list by considering other requirements: processing performance, cost, and so on.

Practices following this protocol will highlight a number of items that should be carefully considered: (1) need to reassess operational procedures when deploying the system, (2) need to set security requirements corresponding to the standardized evaluation method, (3) need to specify information obtained from vendors, (4) need to track requests to furnish information to vendors, and so on. Sorting through these issues and figuring out how best to respond will be fundamental challenges for financial institutions as they incorporate biometric authentication systems.

Notes

[1] The views expressed in this paper are those of the author, and do not necessarily reflect the official views of the Bank of Japan. Analysis and discussion in this paper is based on the following literature: Masashi Une, "Efforts to establish security evaluation methods enabling biometric authentication systems to detect artifact attacks," *Kinyu-Kenkyu*, 35 (4), Institute for Monetary and Economic Studies, Bank of Japan, pp.55-90, 2016 (in Japanese).

[2] Center for Financial Industry Information Systems (FISC), "2015 Financial Institution Questionnaire Results," *Financial Information Systems*, No. 338, FISC, pp.1-289, Oct. 2015 (in Japanese).

[3] The questionnaire was distributed to 873 institutions including city banks, trust banks, regional banks, regional banks II, and other banks licensed under the Banking Act, Shoko Chukin Bank, Norinchukin Bank, Shinkin Banks, Shinkin Central Bank, credit unions, Shinkumi Federation Bank, Labour Banks, Credit Federations of Agricultural Cooperatives, life insurance companies, non-life insurance companies, securities companies, and credit card companies (709 institutions responded).

[4] Financial Services Agency, "Status of countermeasures dealing with counterfeit cash cards (as of the end of March 2015)," 2015 (in Japanese).

[5] In March 2016, Aeon Bank announced a trial service relying solely on a fingerprint to authenticate customers at ATMs (Aeon Bank, "Trial demonstration launch of fingerprint authentication system," March 29, 2016 (in Japanese)).

[6] Security related aspects of FIDO for Internet banking are covered in the following literature: Hidemitsu Izawa, and Hidehito Gomi, "What financial institutions should consider when deploying next-generation authentication technologies: focusing on FIDO," *Kinyu-Kenkyu*, 35 (4), Institute for Monetary and Economic Studies, Bank of Japan, pp.21-54, 2016 (in Japanese).

[7] Takashi Hara, "Vein authentication just using a smartphone camera," *Nikkei FinTech*, Nikkei Business Publications, Inc., May 25, 2016 (in Japanese).

[8] For examples of this work, refer to the following literature: Masashi Une, and Tsutomu Matsumoto, "Vulnerability of biometric authentication systems: focusing on forgery of human physical characteristics," *Kinyu-Kenkyu*, 24 (2), Institute for Monetary and Economic Studies, Bank of Japan, pp.35-83, 2005 (in Japanese).

[9] The project is referred to as: "Project to accelerate strategic international standardization: construction of an infrastructure that promotes international standardization needed to develop a biometric authentication security evaluation infrastructure contributing to cloud security."

[10] Regarding the security evaluation and certification framework in keeping with the Common Criteria standard, refer to the following paper: Yuko Tamura, and Masashi Une, "Third party evaluation and certification schemes for information security products and systems in the financial sector," *Kinyu-Kenkyu*, 27 (1), Institute for Monetary and Economic Studies, Bank of Japan, pp.79-114, 2008 (in Japanese).

Cover Art

Koka Mutamagawa Mutsu Noda
(A woman standing by a river in Tohoku region, one of six popular rivers for composing tanka poems.)

Utagawa Hiroshige (1797-1858)

Collection of the Art Research Center (ARC), Ritsumeikan University
Object number: Ebi0107