NEW SCIENCE
TRANSACTION SECURITY
ARTICLE

BIOMETRICS FOR PAYMENTS

SUMMER 2014
UL.COM/NEWSCIENCE
NEW SCIENCE
TRANSACTION SECURITY
OVERVIEW

From research on the latest electronic transaction security technologies to comprehensive strategies for reliable mobile payment solutions, UL’s New Science advances are helping to support compliance, interoperability and security for the latest transaction technology implementations.

UL is working with customers across the industry, conducting state-of-the-art pilots; analyzing and assessing the security, functionality and interoperability of new and existing technologies; and enhancing implementation processes and developing unique migration architectures to help transition disparate systems to a new platform.
WHY BIOMETRICS FOR PAYMENTS MATTERS

Advances in technology are making payments today more streamlined. Yet, as more personal and financial information are digitized, the risk of theft and fraud is growing. Biometrics — an automated method of recognizing an individual based on their measurable physiological (e.g., fingerprint) and/or behavioral (e.g., gait) characteristics — offers an easy-to-use and convenient means of authenticating users, granting them access to various services. Today, as the price of biometric systems has become increasingly affordable (it now costs less than $7 to install a fingerprint scanner on a mobile phone), these new systems are being released by various industry sectors and the use of biometry is on the rise. Biometrics is important for payments because of its ability to enhance the security of transactions that are becoming more varied in type and less physical in form (e.g., contactless payments and card-not-present Internet purchases).

CONTEXT

Since the 1970s, government and law enforcement organizations around the world have used biometric technologies for border control, fraud security and criminal identification, which has helped establish biometrics as a highly efficient method of identity recognition. Today, other industries, including banking and payments, are increasingly turning to biometrics, which has led to significant growth projections: 114 percent from 2012 to 2015, when biometric revenue is forecast to reach $15 billion, and an additional 57 percent through 2020, when the market will be worth $23.54 billion. The growth of biometrics is largely attributable to a decrease in costs plus enhancements to the technology in terms of additional miniaturization and software optimization that, together, have made this type of security more accessible. The financial services industry is driving much of the commercial demand and is expected to account for more $8 billion, or 34 percent, of the global market by 2020. By using biometrics, financial institutions believe they will be able to provide the level of security necessary to reduce the risk of Internet fraud, money laundering and identity theft, while also reducing operational risks through more efficient and faster transaction processes. Industry projections suggest that biometric security can reduce a financial institution’s operational risk by 20 percent over the next 10 years. This further increases the appeal of biometrics as, on average, one to two percent of daily payments are subject to some form of inquiry or investigation, which accounts for a significant portion of operational costs.

Many banks around the world have already implemented biometrics for customer identification or authentication, in most cases in the form of fingerprint reading. Identification involves the comparison of the biometric traits of one person with all traits stored in a database, in an attempt to establish the identity of an unknown individual by answering the question, for example, ‘Who has this fingerprint?’ This is a powerful method to prevent identity fraud. Authentication is about verifying someone’s identity once they have identified themselves through other means; as
such, biometric authentication can be used as a replacement for a PIN or password, (e.g., at an ATM).

Countries such as Brazil, India, Poland and Japan already support ATM cash withdrawals by means of biometrics, and many other countries intend to follow in the near future, especially in Asia and Africa.

While security experts are cautious about the use of biometrics in the highly regulated banking industry, banks are rolling out these solutions as countermeasures to two common security issues. The first is identity theft, mainly in the form of enrollment fraud, where a customer applies for a bank service or a credit line using a fake ID. The second is increasing fraud at ATMs, especially card trapping, which involves the physical capture of the card and compromised PIN, use of lost and stolen cards; and skimming (in regions that have not migrated to chip and PIN cards), which involves the capture of card details and PINs for use in the production of counterfeit cards.

By implementing biometric systems, a number of banks have managed to reduce losses due to identity theft to a level that justifies the business case for implementation. One of the popular methodologies now used by banks to ensure that no applicant is registered twice is the Automated Fingerprint Identification System (AFIS), originally implemented by the FBI for criminal cases. Once a bank has stored the biometric data of its account holders in a database, it can also use biometrics for authentication when authorizing transactions. In this way, a bank can safeguard against skimming or misuse of lost and stolen cards at ATMs while protecting itself against potential liability for withdrawals denied by the cardholder.

For the payments industry, the value of biometrics lies in its potential to facilitate secure cardless payments. Environments for which biometrics could prove relevant include online payments and retail.

A considerable amount of fraud exists with Internet-based payments, exacerbated by a lack of robust customer authentication mechanisms. The use of biometric authentication could add a new level of assurance to e-commerce transactions by ensuring that usage of a payment card is restricted to its legitimate owner. One early example is the Samsung Galaxy S5, which made it possible to use fingerprint authentication for payments via any app or website that accepted PayPal. With the swipe of a finger, consumers could log into their PayPal accounts, which is convenient and offers an extra layer of security to the transaction.

In retail environments where Near Field Communication (NFC)-based or Bluetooth Low Energy (BLE)-based payments are accepted, biometric authentication at the point-of-sale could conveniently provide a second layer of security to protect the user. In some cases, biometrics could enable a shopper who has an account with a retailer to pay without using a credit card or a mobile phone. For customers who carry too many cards and have difficulty remembering different PIN values, biometrics would enable them to complete transactions. Beyond the simplicity of authenticating by placement of a
Fingerprint recognition is still the leading biometric solution, but methods that are more difficult to forge are gaining popularity.

There are obvious benefits to biometric security. However, UL believes it is important to better understand the strengths and weaknesses of biometrics as well as the contexts in which it is most appropriate today and where its use might warrant further development.

WHAT DID UL DO?

UL performed a detailed investigation of biometric security to identify potential security issues specific to current and potential near-term usages of the technology by the banking and payments industries. Our analysis yielded insight into the risks involved with hardware, biometric data and standardization that led us to conclude that biometrics requires maturation in these three areas.

Security and reliability of the biometric device

Shortly after the release of the iPhone 5S, it was possible to fool the fingerprint scanner by copying the fingerprint of the owner and creating an artificial or “gummy” finger that could be used to unlock the device. Fingerprint readers used by ATMs are typically equipped with more sophisticated modules to perform Live Finger Detection (LFD). Many of them use multi-spectral and multi-polarization analyses to detect whether the fingerprint provider has the physical structure of a real finger. However, LFD is not an exact science.

The reliability of a fingerprint scan represents a trade-off between the False Rejection Rate (FRR) and the False Acceptance Rate (FAR). FRRs produced by a scanner will provide an unsatisfactory consumer experience, but a less finely tuned scan would be more vulnerable. The relationship between the FRR and FAR depends on a variety of factors, for which there is no current standard, with models still subject to scientific experimentation and proof-of-concept testing. However, experience has shown that the FAR can be increased by fraudulent attacks. Every year, more sophisticated attacks are published, and better readers and LFD modules are developed. This is good news but is also a warning sign. Although most of the implementations in the banking industry still rely on a fingerprint as the primary biometric characteristic, the vein structure of hands and fingers is gaining popularity, as it is an equally convenient method but much more difficult to forge than a fingerprint. Also, vein recognition technology tends to have a much lower FAR than fingerprints. Other biometric methods, such as face recognition, are also gaining popularity. Similar to the fingerprint, it is possible to integrate this method in a smartphone. Some models are already being released with multiple front cameras, which enable a more reliable facial recognition assessment.
Particularly if stored on a central database, biometric data may be at risk of being compromised.

Security of biometric data
Most media and academic attention are paid to the falsification of the biometric trait, such as the replication of a fingerprint. But after this information is captured, the trait is transformed into digitized data. This raises the question about how digitized data are protected. If criminals can make a “copy” of the data, they can pose as the person providing it. Although there is a strong history and culture of physical and logical security for PINs and card data, this is lacking for biometric data. Furthermore, one of the reasons why the financial industry in developed countries is not ready to adopt biometrics is due to the need to comply with strict personal data protection regulations, such as the European General Data Protection Regulation (GDPR). The risk of compromise of this information stored in a centralized database is real and unacceptable to security officers of many banks. The liability arising from data leakage due to an attack is also difficult to estimate.23

There have been repeated attacks on payment systems recently. One example is the breach of credit card data of 40 million customers of the American retailer Target in 2013.24 Aside from dealing with the financial loss, banks react to such breaches by reissuing customer credit cards. In the case of biometrics, however, the customer fingerprint cannot be reissued. Furthermore, some banks store the full biometric data in their databases, not just the trait or template. This is done to avoid vendor lock-in (i.e., a lack of flexibility to change vendors), because the template is vendor-dependent but the fingerprint is not. A compromise of a fingerprint database could affect customers in all government and industry sectors that rely on biometrics, which would pose a threat of unpredictable liability.25

One important step toward ensuring privacy while also mitigating the risks of centralized databases would be to give control of the biometric data to users. The biometric feature template would be stored in a safe place controlled by the owner rather than in a centralized location. This “safe place” could have different form factors, ranging from a card to a key fob or mobile handset. It would be important to safeguard access to the biometric factors in the consumer device as well.26 Apple’s Touch ID fingerprint sensing system, for example, includes user-controlled biometric data. The microchip that powers the technology is equipped with a secure coprocessor (named “Secure Enclave”) that makes possible an isolated treatment and computation of the data and related operations in the handset itself. Also, through strong cryptography, all communication between the Touch ID fingerprint system and the Secure Enclave is protected, rendering any interception of the data worthless.27

Lack of standardization
Standardization of the representation, interoperability and quality of biometric data has improved in the past few years, as standardization bodies, such as the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST) and the British Standards Institution (BSI), regularly release...
biometrics standards, although there is no standard way, recognized industry-wide, to validate the security of biometric data for payments. There are organizations that provide validation of biometric solutions, but today, the methodology and security requirements lack the same degree of scrutiny of those traditionally used by the payments industry. Because a biometric system can only be as secure as its weakest link, security standards and evaluation need to cover the whole chain, including service enrollment, usage, transmission and storage of biometric traits as well as all devices involved in this process.²⁸

The lack of standardization can be a barrier to interoperability, especially in an ecosystem where multiple players need to be integrated. There are, however, important new industry initiatives to tackle these needs. In particular, the Fast IDentity Online (FIDO) Alliance, an industry consortium, is developing open specifications for strong universal authentication. This would allow technologies such as biometrics to be used in a common interoperable way. One of the main goals of this initiative is to supplant the reliance on passwords to securely authenticate users of online services by supporting a full range of technologies, such as fingerprint and iris scanners and voice and facial recognition devices. The major payment schemes have joined the FIDO Alliance along with leading technology companies and banks. UL believes this widespread participation and recognition are essential to achieve the successful adoption of a new set of standards.²⁹

IMPACT

At UL, we think that, despite its clear benefits and broadening applicability, biometric security needs further development to enhance its appropriateness across the full range of payment applications for which it is being considered. For example, the use of biometrics requires different approaches for customer identification and authentication. Identification involves the comparison of one biometric reference to many references stored in the system (1:N), which gives the FAR an important role. On the other hand, the use of biometrics to authenticate a customer requires the comparison of one biometric feature to just one reference feature stored in the system (1:1), as the customer has already been identified through other means (e.g., by inputting a correct PIN code), which makes the FAR less important and the FRR more so. With banks and payment schemes implementing a wide variety of biometrics system architectures and designs, a comprehensive set of standards is needed for security and testing. We believe the establishment of industry-wide standards is a fundamental step in the maturation of biometrics. We see the role of this technology continuing to expand as new and more complex banking and payment transaction applications are developed, and individualized identification, authentication, access control and security increasingly required.³⁰
SOURCES

12. Ibid.
13. Ibid.
16. Ibid.
17. Di Lorenzo, H., Interview, UL, 26 June 2014.
18. Ibid.
21. Ibid.
22. Di Lorenzo, H., Interview, UL, 26 June 2014.
29. Di Lorenzo, H., Interview, UL, 26 June 2014.
TRANSACTION SECURITY ARTICLES

MOBILE PAYMENTS

SECURING HCE

MOBILE PAYMENT SECURITY: BLE OR NFC

SECURE PAYMENTS

BIOMETRICS FOR PAYMENTS

TRANSIT TICKETING

CONTACTLESS INTEROPERABILITY IN TRANSIT

NEXT GENERATION TRANSIT TICKETING
NEW CHALLENGES. NEW RISKS.

NEW SCIENCE

To learn more, explore the New Science of Indoor Air Quality, Transaction Security, Sustainable Energy, Workplace Health & Safety and Fire Safety. Watch our videos, read our journals, articles and case studies, scroll through our galleries and meet our experts.

VISIT US ON UL.COM/NEWSCIENCE

NEWSCIENCE@UL.COM
+1 847.664.2040

New Science Transaction Security cannot be copied, reproduced, distributed or displayed without UL's express written permission. V.14.

UL, the UL Logo and NEW SCIENCE are trademarks of UL LLC © 2014.