EL MUNDO
ARIADN@

02/25/2007

Biometrics to combat card cloning

A study published last week ranks Spain number two in Europe in the production of fraudulent credit cards, at over two million per year. Spanish banks are now looking into identification systems to enhance security.

ANGEL JIMENEZ DE LUIS

It's not terrorism, nor job loss nor global epidemics - Spaniards' greatest worry, according to a survey by VISA, is the theft of their personal and financial information. Approximately 64% considered such identity theft to be the greatest threat to our modern world, compared to 58% who fear being the victim of an attack by an armed group. The truth is that, according to the company Xelios Biometrics (a part of the French group Sagem) there are over two million cases per year of bank fraud. Some studies rank Spain number two in Europe in this type of crime, and figures from the Bank of Spain and various financial associations show that the problem is growing. We are currently host to a little less than 10% of crimes related to credit and debit cards in Europe, at 22 million cases per year.

BIOMETRICS. The criminals that engage in credit card fraud have very sophisticated technology. In their search for a solution, banks are turning to technology that they have largely neglected for many years: biometrics. European demand fo biometric technologies in the financial self-service channel is low, said Santiago Perez-Bedmar, director of marketing for financial institution Iberica NCR. However, since the 90's the bank has experimented with different solutions to combat card fraud. Before its merger with BBV, Iberica's Argentinean branch launched a pilot of ATMs equipped with identification by iris, the safest biometric technique, Perez-Bedmar adds.

Today, banks opt for solutions that detect attempts to modify or copy elements installed in ATMs. One example of this is NCR's Intelligent Fraud Detector, a set of security solutions to discover changes in the environment of the machine and notify an entity of, for example, the installation of cameras to record the keypad area of the ATM.

Biometrics are providing a major boost in the financial security market, especially in the Southeast Asia and Latin America market. Last year the Osaka Senshu Bank, for example, began issuing credit cards embedded with customers' palm and fingerprint data. Sugura Bank, another Japanese company, launched a network of ATMs with biometric identification where the customer only has place his/her hand to be identified - no card required. Colombia is another country where fingerprints are used to withdraw cash. Bancafe, the fifth largest Colombian bank, deployed 500 kiosks in 2004 that are equipped with a fingerprint reader to eliminate the need to carry credit cards in one's wallet.

The use of an identification card with an embedded biometric will put an end to skimming attacks. 70% of banks are working on projects to launch safer ATMs with better anti-fraud measures, says Francisco de Asis Romanan, president of Xelios Biometrics in Spain.

HANDS. Several different biometrics can be used to identify users, including the scanning of various body parts and even a person's voice or gait. Fingerprint reading is the most widespread; many readers are probably already familiar with fingerprint identification systems that act as a "master key" to remember the many passwords that we face every day. Fingerprint readers have also been implemented in a variety of services. Some amusement parks, for example, employ biometrics to ensure that an individual buying multi-day passes is the same person *using* the passes. Some fingerprint systems can be spoofed with a fingerprint mold or even a photo, but the most advanced solutions incorporate safeguards such as body heat or blood flow detection to ensure that a finger belongs to a live person and is not a mold or an amputated finger.

It is also possible to identify a person by the geometry of the hand. Hand geometry offers the same reliability as fingerprint recognition and is sometimes easier to use, since a user can simply rest his/her hand on a flat sensor.

> Safest. Iris identification is the most reliable biometric technique, but requires the user to be familiar with the scanning procedure and present his/her eye to a camera. Fingerprint recognition is easier and more intuitive, which is why it's already a common feature in some laptop computers.

FACE. Our faces make us unique, in more ways than one. The face contains an individual's most distinct features it's usually visible, so it's an excellent biometric identifier. Facial recognition systems work by measuring various parameters such as the shape of a subject's jaw, the distance between his eyes, the thickness of his lips or even the texture of his skin. Measurements can be performed on a two dimensional picture or a three dimensional facial image.

However, the most accurate biometric technique right now is iris identification. Each iris is unique and extremely hard to duplicate. The downside is that iris identification requires cooperation from the user, who must approach a camera and sit still during the scanning process. Iris recognition is commonly confused with retinal scanning, in which a laser is used to scan and analyze a user's retina. Retina recognition is considered one of the best biometrics, but also has the least popularity among users, both because of the need to approach a special reader and also because it's slower than iris recognition.

GESTURES. Finally, some universities and companies are studying other forms of biometric identification that do not require active user participation and my even work without the subject noticing. The analysis of hand movement during a signature is one example, or the identification of an individual by his walking gate or the sound of his voice. Even the way a person types can provide answers to his identity. A research team from the Massachusetts Institute of Technology has recently managed to identify a user sitting at a computer just by analyzing how a person types and how much pressure he applies to various keys.