ELSEVIER

biometric TECHNOLOGY TODAY

ISSN 0969-4765 October 2011

www.biometrics-today.com

FEATURE

Mobile Payments, Digital Wallets and Tunnel Vision

by

Kenneth Weiss, USR

Kenneth Weiss, USR, examines the security implications of using biometrics to authenticate payments via mobile devices.

Mobile payments, digital wallets and tunnel vision


Kenneth Weiss

Kenneth Weiss, USR

Convenience, versatility, and benefit to the consumer are the keys for the acceptance and success of a new technology. Imagine conveniently authenticating your identity to your mobile phone, with reliable three-factor security incorporating biometrics, at the beginning of your day, and having doors automatically unlock as you approach, security alarm systems go into standby mode when you enter your home or office, your computer being active and unlocked only while you were sitting in front of it (with your mobile phone), and paying vendors, vending machines, or individuals, directly or with credit from your mobile phone.

However introducing biometrics as a factor is not enough on its own to ensure the security of mobile authentication. There must be a move away from storing and transmitting sensitive account number and PIN information if biometrics are to meet their potential as a means of mobile authentication.

As credit cards have become ubiquitous, so has counterfeiting and fraud. Magnetic stripes with recorded account numbers and other private information were added to raise both the threshold for counterfeiting and to expedite transactions at the point of sale (POS); unfortunately with some simple tools easily purchased, these cards too were counterfeited and abused. In response the industry introduced multi-band magnetic stripes. Abuse continued.

"Other measures to help stem the tide of abuse have been employed – signatures, second factor, biometric and personal identification numbers (PINs) as a third factor 'secret' and some encryption. Theoretically, these additions decreased abuse because they created two or three-factor security. Abuse continued"

Other measures to help stem the tide of abuse have been employed – signatures, second factor, biometric and personal identification numbers (PINs) as a third factor 'secret' and some encryption. Theoretically, these additions decreased abuse because they created two or three-factor security. Abuse continued.

Security factors

There are only three underlying means or factors by which people can identify themselves: something relatively uncounterfeitable (a token), something not public and obvious, known only to the individual (a secret) and a physical characteristic (a biometric). If properly implemented, their relative security can be multiplied together for statistically undefeatable identity authentication.

As universal use and the popularity of credit cards accelerated, abuse accelerated. Eventually holograms were added to strengthen the core 'token' and to further reduce the vulnerability to counterfeiting. Plastic sheets of hundreds of counterfeit credit cards with holograms, many produced in Hong Kong, became available on the black market.

Tunnel vision

Now, near field communication (NFC) is being touted with the false promises of being a secure solution and offering faster transactions. However, fraud, and exploitation are possible by the clandestine use of sensitive receivers or wiretapping to harvest the sensitive information now radiated from the NFC chips.

The problem continues to be the industry's tunnel vision. All of the improvements cited above are reactive and linear; no one has bothered to think outside the box. For a credit/debit card transaction all that is necessary at the point of sale is that the user must be reliably identified. Storing an account number and a PIN in a card, or, as is now being proposed, in a mobile phone, and then radiate it does not address the issue of how to identify an individual at the POS reliably without compromising or exposing any exploitable information.

Only the remotely located issuing bank needs to see and use the private account number. PINs and account numbers need never be exposed, in any form, at the POS or stored in the digital wallet.

SecurID

Twenty five years ago a similar problem was solved with the invention of the SecurID token and its more secure cousin, the Pin Pad card. With the Pin Pad SecurID card, invented and patented by author Kenneth Weiss, the user enters a PIN on a touch pad on the SecurID card which then xors the pin with the next pseudo random number, (PRN) and displays the result as a decimal number, which can then be entered as a passcode to create two-factor identity verification at a remote computer.

Xoring refers to the mathematical process that in binary arithmetic it is axiomatic that a constant added to a random binary pattern, without carry, produces a random result. When the initial random pattern is added to the result of this arithmetic, the constant is exposed.

The challenge was the same then as it is now. How does one reliably authenticate her/his identity to a remote computer employing two-factor identity authentication in a way that cannot be exploited and provides no useful information which can be usurped, observed, replayed or otherwise compromised?

The answer then was to provide an individual with a token that generates a different pseudo random number (PRN), unique to that token, every minute and generate the same codes remotely, synchronised in time, at a protected computer. A user's PIN can be entered

on the device and xored to the PRN stored in the mobile device. The process assumes that both the mobile device and the remote server are independently generating the same PRN synchronised in time The PIN need not be stored in the device and is never radiated.

At the remote protected computer the authorised user's PRN is also generated and that authorised user's PIN is xored to it; if there is a match, then the user's identity has been reliably verified by two factors. When the one-time PRN is observed or radiated it has no value to anyone except the authorised user and cannot be compromised.

Discussions about the nature and location of the secure element on a mobile device enabled for payments become largely academic with this approach. Nothing that can potentially compromise an individual is stored in a mobile phone and nothing of value is ever radiated.

Biometric perspective

A modern mobile phone is an exceptionally desirable platform to exploit and benefit from user friendly and meaningful three-factor identity authentication. Today's mobile phone platform, without hardware modification, is appropriate for several biometric modalities such as voiceprint and facial recognition.

"Today's mobile phone platform, without hardware modification, is particularly appropriate for several biometric modalities such as voiceprint and facial recognition"

Many believe that use of a biometric is the Holy Grail for reliable and secure personal identity authentication. A circumstance-specific properly implemented biometric is a critically valuable component of reliable, secure identity authentication. But if not calibrated to the circumstance or if used alone it is dangerous false security. Some of the special considerations around automated biometric analysis are:

TYPE 1 error: In the context of a biometric, this is the percentage of times the correct target individual is falsely measured not to be the actual target. For example with a voice biometric, because of having a cold or congestion, background noise, emotion, or rate of speech an individual does not sound like her or himself.

TYPE 2 error: Without getting into a technical discussion of statistics and assumptions associated with rejecting the null hypothesis; simply stated in the context of a biometric, a type 2 error is the likelihood that someone other than an authorised target individual will be identified in error as that individual. For example a type 2 error of 1/10,000 means that one person in 10,000 may be falsely measured and be identified as the target individual.

The more stringent the type 2 measurement standard eg 1/20,000 the higher the rate of type 1 errors, 20% (one in five times), when you do not sound like yourself. Obviously for appropriate security the type two threshold must be set to circumstance specific levels to insure reasonably security with reasonable convenience.

Another factor is how to respond if the security factor is compromised. If one's PIN is compromised it can be changed; if a token is lost, stolen or counterfeited it can be replaced. If however, for example, your fingerprint is captured you can't replace your finger.

The appropriateness of the biometric is key. Meaningful circumstance-dependent choice of an appropriate biometric and calibration of the type 2 error, with consideration to an acceptable type 1 error must be responsibly implemented.

For example at the point of sale a cashier-evaluated facial recognition is more appropriate than a cashier-evaluated signature or fingerprint.

Paradigm shift

USR's mobile phone app provides a model of how biometrics may be used to authenticate payments securely. It provides one-factor security through a tamperproof electronic serial number and a discrete binary pattern. An individual is required to enter a PIN (secret, factor two) and speak (voice biometric, factor three) a short series of numbers or characters displayed on the mobile phone. These characters are presented and displayed each time in a different random sequence. This operation need only occur once a day in a relatively quiet environment.

Once the mobile phone is activated, for a user-selected period of time, it can be used for a wide range of secure financial transactions. When the mobile phone is in close proximity to the point of sale at a co-operating vendor, a wireless dialogue between the mobile phone and a module at the point of sale takes place. Depending on the situation, this dialogue can be NFC or Bluetooth. The app generates and sends a 16 digit one-time use, pseudo random number, and a code for the preferred payment method. These are combined at the POS with the merchant code, amount of purchase, etc. and this one-time PRN.

A remote computer receives this PRN representing the satisfaction of the personal identifying factors which, if valid, matches during this time period to a particular authorised user. The user's remotely and securely stored account number and transaction details are sent to the credit issuing bank or transaction processing facility, and a stored digital picture of the individual is sent by USR to be displayed at the POS. This entire process with a second biometric, the picture, represents 3+factor security and takes place in a fraction of second.

Locked in an outdated paradigm some companies are experimenting with alternating or encrypted the account number alongside introducing a biometric. However, in most implementations alternate or encrypted account numbers can be exploited and replayed or decrypted. Even circumstance or time-modified encryption contains information that may be decrypted. The mobile device still retains the sensitive information and it can be compromised.

NFC standards

Currently there is a frenzy of activity, with hundreds of companies testing different strategies and evaluating standards for NFC associated with financial transactions. Prominent among these are a consortium called Isis, the major credit card companies, and Apple, Google, etc.

This new technology must be robust enough to facilitate the ushering in of a cashless society. If the radiation, in any form, of an individual's account number, PIN, or any other sensitive, private, or exploitable information becomes common we will be creating an environment for a tsunami of abuse, fraud, and identity theft disproportionate to any abuse previously experienced.

Many poor ideas are being considered for mobile funds transfer because credit card fraud and abuse represents a small percentage of the costs of the banking sectors. The actual losses are passed on to the vendors and cardholders and it's your identity at risk not theirs.

Complacency must be replaced by a responsible solution that can promote an enduring technology that is in the interest of the consumer and society. This is an opportunity to create open standards that will reliably propel us into the future with a broad range of potential applications that will provide both strong security and convenience going forward.

About the author

Kenneth Weiss founded Security Dynamics in 1984, and as its CEO invented the SecurID token. He authored 17 patents, which represented the core technology when he brought the company public on NASDAQ in 1994, and achieved a $4bn market capitalisation. SecurID is a trademark of RSA the security division of EMC.