April 6, 2012

Tunnel Vision and Mobile Payments (White paper)

by Kenneth P. Weiss

Source: Universal Secure Registry

Date: April 2012

Type: White Paper

Overview: In this contributed article the author will first briefly set the stage with the evolution of the credit card industry bringing us up to speed with where it is today. Weiss contends that consumers and retailers alike are stuck in the past with tunnel vision when it comes to securing mobile payments. Next, Weiss will identify the reasons why many of the players in the market aren't as concerned as they should be including:

1) NFC - It's being touted with the false promise of a security solution and faster transactions.

2) Encryption - In most implementations, an encrypted account number can be exploited and replayed or decrypted.

3) Assumed losses - Credit card companies? business models assume loss and margins allow for it. They don't need proactively implement a solution.

Weiss proposes that the solution is implementing a technology that can reliably identify an individual at the POS, without compromising or exposing any exploitable information. Only the remotely located issuing bank needs to see and use the account number.

http://banktech.com/whitepaper/Payments-Cards/Wireless-Mobile/tunnel-vision-and-mobile-payments-wp1333489151?articleID=191704464

PERSPECTIVE: MOBILE PAYMENTS and LEMMINGS

(A definition of insanity is doing the same thing over and over and expecting different results)

Kenneth P. Weiss

I remember as a child my mom producing from her change purse a charge plate at the cash register of a department store. The charge plate had her name, account number, and issue date embossed on it. It looked like a metal GI dog tag. The clerk imprinted the charge plate on a cash register receipt and she received a bill at the end of the month. The possession of this charge plate with its embossed information identified my mom as a regular customer and was reasonable security for these limited circumstances in a kinder, gentler age.

PERSPECTIVE

A few years later, the plastic credit card emerged with the same information embossed on it, but now for wider use across multiple vendors. This was a transformational business model. Along with the higher value of the embossed information on the cards, counterfeiting, stolen account numbers, fraud, and identity theft emerged. As the cards became more ubiquitous, so did counterfeiting and fraud. Magnetic stripes were added to raise both the threshold to counterfeiting and to expedite transactions at the point of sale (POS) Unfortunately with some simple tools easily purchased at any Radio Shack, 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, personal identification numbers (PINS), and some encryption were added. Abuse continued. Theoretically, these additions should have decreased abuse because they created two or three-factor security.[i]

As universal use and the popularity of credit cards accelerated, abuse accelerated. Eventually holograms were added to further reduce the vulnerability to counterfeiting. But plastic sheets of hundreds of counterfeit credit cards with holograms, many produced in Hong Kong, became available on the black market; abuse also increased. Like lemmings to the sea most players in the mobile payments industry are following each other in a limited and inappropriate direction. No one has bothered to stand back and re-conceptualize the problem, and as a result, solutions, even today, have been reactive instead of proactive, tunnel vision.

The pachyderm previously present persists. All of the aforementioned approaches exposed the name of the consumer and account number. Now near field communication (NFC) is being touted with the false promise of a security solution and faster transactions. However, even with NFC as proposed, sensitive information is radiated, and abuse, fraud, and exploitation are possible through the clandestine use of sensitive receivers, hacking, or wiretapping to harvest that sensitive information radiated from the NFC chips. Sophisticated abuse will likely be facilitated!

TUNNEL VISION

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 POS is that the user must be **reliably identified**, period. It is a cockamamie solution to store an account number and a PIN in a card, or, as is now being proposed, in a mobile phone, *and then radiated*! The real issue is how to reliably identify an individual at the POS without compromising or exposing any exploitable information.[ii] Only the remotely located issuing bank needs to see and use the account number. PINs and account numbers need never be exposed, in any form, at the POS or stored in the digital wallet.

RELIABLE IDENTITY AUTHENTICATION

Twenty−five years ago a similar problem was solved with the invention the SecurID token and its more secure cousin, the Pin Pad card[iii]. The challenge was the same then as it is now: how does one reliably authenticate her/his identity to a remote computer employing, *meaningfully*, at least 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 successful answer twenty−five years ago was to provide an individual with a token that generates a different pseudo random number (PRN), unique to that token, every minute and to generate the same codes remotely, synchronized in time, at a protected computer. A user's PIN can be entered on the device and xored[iv] to the PRN. The PIN need not actually be stored in the device, *and never radiated*. At the remote protected computer the authorized user's PRN is also generated and that authorized user's PIN is xored to it; if there is a match, then the user's identity has been reliably verified by two factors. The privileges associated with this user are then available. This reliable and proven technology never has been defeated. If the one time PRN is observed or radiated, it has no value to anyone except the authorized user and therefore cannot be compromised.
This strategy for strong two-‐factor security in the form of SecurID tokens for computer and network access was patented in the late '80s.[v] By leveraging this undefeatable technology with a new focus for mobile transactions and a series of transformational enabling patents, Universal Secure Registry (USR) was founded. Mobile industry discussions about the nature and location of the so-called "secure element" on a mobile device enabled for payments become largely academic with the USR approach. Nothing that can potentially compromise an individual is stored in a mobile phone equipped with a USR app, *and nothing of value is ever radiated*.[vi]

UNIQUE OPPORTUNITY

A modern mobile phone is an exceptionally desirable platform to exploit and benefit from user-friendly and meaningful three−factor identity authentication. A software application (app) downloaded into a mobile phone is already a discreet token (token, factor one) with its unique tamper-proof electronic serial number and with the USR patented app's discreet binary pattern. With a USR app an individual is required to enter a PIN (secret, factor two) and speak (voice‐biometric, factor three) a short series of numbers[vii] displayed on the mobile phone. This operation need only occur once a day. 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 (POS) at a cooperating vendor, a fully automated wireless dialogue between the mobile phone and a module at the POS takes place. Depending on the situation, this dialogue can be via NFC or Bluetooth. The USR 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 3 personal identifying factors which, if valid, matches during this time period to a particular authorized 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 a second.

Locked in the outdated traditional paradigm (tunnel vision), some companies are experimenting with encrypting the account number. However, in most implementations an encrypted account number 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.

LEMMINGS

Currently there is a frenzy of activity associated 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, Apple, and Google, etc. The slavishly adhered to local exposure of the account number must be abandoned, the problem reconceptualized, and a standard created that is more than a temporary solution. 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.

A LESSON WELL LEARNED

In the early 90's after I had for several years been an invited and featured speaker at the American Bankers Association convention, I was asked to dinner by a senior executive of the association. He asked how many SecurID tokens I had sold to bankers; I told him none yet. He offered to tell me why. He said there were three reasons: 1. Banks were insured, 2. If a bank used different or even stronger security than that which had been approved, and there was a security breach (even unrelated to the SecurID token), they likely would not recover because of using a non-recommended technology, and 3. "It's your money at risk, not ours." I had been naive; I had an epiphany!

He offered to champion the SecurID for approved and recommended status. He did, and today it is still the preferred product for use in that environment. This anecdote may help to explain why so many poor ideas are being considered for mobile transactions. Credit card fraud and abuse represents a small percentage of the cost of conducting this profitable business. The actual losses are passed on to the vendors and cardholders[viii], 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. We must embrace the challenge as an opportunity, put aside politics and special interest, tunnel vision, and choose the best comprehensive and enabling technology. 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.

Convenience is the key for acceptance and success of a new technology. Imagine conveniently authenticating your identity to your mobile phone with reliable 3 factor security 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, and paying vendors and vending machines or individuals directly or with credit from your mobile phone. These are only a few of the possibilities enabled by USR technology.

###

NOTES

[i] There are only three means by which people can identify themselves: Something relatively uncounterfeitable possessed (token), something not public and obvious known (secret) and some characteristic a physical measurement (biometric). These are the three factors. Their relative security can be multiplied together for statistically undefeatable identity authentication. The signature required on the back of a typical credit card was a reasonable attempt at an inexpensive biometric factor to add to the first factor, which is the credit card itself, or token. However, in practice, it is almost meaningless, usually not even looked at, and when not ignored, relies on the absurd premise that a cashier has expertise in analyzing handwriting. The potential use of a secret PIN is inconvenient and rarely used at all in the U.S. Therefore, in practice, a credit/debit card is a single factor token that exposes sensitive information and can easily be abused.

[ii] The merchant number, amount of sale, etc. can be sent in the data stream to a remote site and does not compromise the individual. However, this information can be also be xored to the string of PRN's for added security and separated (xored) at the remote USR server.

[iii] The Pin-Pad SecurID card, invented and patented by Weiss, is the most secure SecurID token because the user enters in PIN on a touch pad on the SecurID card which then xors the pin with the next PRN and displays the result as a decimal number, which can then be entered as a passcode to create 2-factor identity verification at a remote computer.

[iv] Xored refers to the mathematical axiom that in binary arithmetic, 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. USR uses this technique to send information such as a PIN from a mobile phone to a remote secure server. The PIN, secret factor, can then be validated. The PIN is not stored in the mobile device. The process assumes that both the mobile device and the remote server are independently generating the same PRN synchronized in time. This technology was invented and patented by Weiss.

[v] Kenneth P. Weiss founded Security Dynamics in 1984 and, as its CEO, invented the SecurID token. He authored the 17 patents which represented the core technology when he brought the company public on NASDAQ in 1994, and achieved a $4 billion market capitalization. He was the largest individual shareholder when he resigned in 1996. More than 100 million individuals, consumers, >90% of fortune 500 companies, banks, governments, and more than 30,000 organizations in more than 30 countries worldwide rely on the core SecurID token technology. In 25 years the SecurID technology has never been breached.

[vi] To the extent the large pseudo random unique binary seed can be considered "sensitive," the USR server, as a background operation, can randomly, remotely, routinely, automatically alter it. The fact that the embedded seed is always modified by a user's xored PIN renders its compromise academic.

[vii] Each time an individual authenticates her/his identity to the mobile phone with a USR app, a short series (6-9) digits is displayed to be spoken for voice analysis; a biometric. These numbers are pseudo random and different each time. The voice recognition technology analyzes the spoken number character by character. This patented approach effectively foils attempts to record or replay any overheard numbers.

[viii] In addition to the interest rates charged to consumers and the percentage of each transaction paid by the vendor, tax dollars also pay for the U.S. Secret Service who assumes the responsibility to investigate and prosecute credit card fraud. This arrangement for the credit card industry reduces motivation to improve security.

SecurID is a trademark of RSA the security division of EMC.

###

