

## **Cell Phone Based Payment Authentication System**

By Ryan Morlok, April 25-26, 2004

The idea is for a system to make payments via a small, electronic device with wireless capabilities, such as a cell phone. The device can either have local wireless abilities (such as Wi-Fi or Bluetooth) or ideally global wireless technologies such as cell phones. Ultimately, the goal is to replace credit cards with a new method of payment authorization, however in the short term this technology could be used to augment the security of existing credit card payment systems with the addition of no new hardware, on either the customer's side (the individual making a payment), or the vendor's side (the store from which the purchase is being made) or on behalf of the credit card provider.

The purpose of this technology is to reduce the occurrence of fraud related to credit cards. In this system, the mobile computing device with wireless capabilities (hereafter referred to simply as a cell phone, as a cell phone like device is likely to be the first incarnation of such a product) is used as a personal gateway to all credit card authentications for a given individual.

In the credit card payment system, a customer gives the vendor his or her card. The vendor then swipes the card with a device which communicates with the credit provider, communicating that a sale is requested, and ensuring that the customer's card has enough credit to cover the purchase. If the customer has enough credit, the purchase is authorized and this ends the initial communication with the credit provider, until a later time when the day's (or weeks) receipts are communicated to the credit provider for payment. A receipt is generally printed out for the customer to sign. The signature serves as proof that the customer is authorizing this transaction.

The problem is that not all transactions require a signature, and those that do are not careful enough in checking to make sure the signature is valid. For example, an online transaction will simply take the card number and post the bill to the customer's card. The fundamental problem with the current system is that only a limited amount of information is required to make a purchase with the card. Generally, the card holder's name, the credit card number, and the expiration date are all that is required to make a purchase with a card, and what's more, all of this information is available on the card itself. This means that the card is physically stolen, or if the information is simply copied from the card, transactions can be made without the authorization of the card owner.

The new system is designed to require the card holder's authorization for every transaction. In this new system, the cardholder still has a credit card as he or she did before. To make a purchase, the cardholder gives the card to the vendor, and the card is swiped as before. This part of the transaction is identical to what has been used in the past. At the authorization stage of the transaction, however, things differ. After the card has been swiped, and before the credit provider will return that it is authorizing the transaction, the credit provider will contact software running on the cardholder's cell phone to authorize the transaction.

This transaction authorization is done by the following: every card holder's cell phone contains a private key. This private key is part of a public, private key pair, which the customer's cell phone can generate. The public key of this pair is registered with the credit provider through a secure means, such as the credit provider's website. When the credit provider wishes to authorize a transaction, the credit provider sends a digital receipt to the card holder containing information such as a unique transaction identifier, the amount of the purchase, the vendor to which the payment will be made, and the date/time of the transaction. In order for the credit provider to authorize a transaction after a card swipe, it must receive this exact same digital receipt back from the cell phone, signed with the private key of the cardholder. Because the credit provider has a copy of the cardholder's public key, it will be able to verify the digital signature on the receipt.

On the cell phone side, the customer authorized a transaction as follows. The cell phone receives the digital receipt from the credit provider and notifies the cardholder that attention is required. The cardholder can then view the details of the receipt. If the cardholder wishes to authorize the transaction, a pass phrase (or simply a pass code) is entered via the keypad of the device. This pass phrase is used to decrypt the private key, which is then used to sign the digital receipt. The private key is stored in the memory of the cell phone in an encrypted form, so that if the cell phone is lost or stolen, it cannot be used to authorize transactions without the pass phrase to decrypt the key.

This technology could be implemented progressively, with customer's opting in if they have the appropriate user technology (the needed cell phone type). Currently, phones exist which run Java Micro Edition, which would be an ideal platform for such a client technology, however it is by no means required. Many phones today allow for the download of software, and this capability may provide the needed interface for the software to be installed.

Credit card companies would simply add a step in their authorization process. Currently, when a store (vendor) wishes to authorize a credit card, they swipe the card and wait for the credit provider to authorize use of the card. It is during this authentication phase that the cardholder would be contacted via the cell phone interface. Once the authorization was complete with the cardholder, the credit provider would return the authorization to the equipment at the vendor's location, and the transaction would proceed as it always had (minus the need for a physical signature). No change in equipment would be necessary at the vendor's location. The only change in credit provider's equipment would be the addition of software to request the signature of the digital receipt from the cell phone, and to verify the signature upon the information's return. This would require some additional processing, however it would not be a substantial change.

The key point to this technology is that no easily obtainable information can be used to gain access to a cardholder's line of credit. The credit card number, the cell phone with encrypted private key, and the card holder's pass phrase must all be in use to authorize a

transaction. Furthermore, vendors cannot be fraudulent because cardholders are authorizing specific transactions with specific transaction amounts associated with them. There is no way for a vendor to overcharge. This technology works equally well for online vendors as well as physical ones such as typically consumer stores. This technology could be applied equally well to transactions involving credit cards as to electronic checks, used by banking systems.

It should also be noted that at no point is any critical information transferred electronically that could be used to hijack account information. The vendor sends the credit card number along with the required payment amount to the credit provider. This information is currently sent, and it could be done over an encrypted line (if it is not done so already) regardless, the card number itself is not enough to authorize a transaction. The information sent to the cell phone of the cardholder is also transaction specific. This information is only useful to the transaction at hand, and does not contain any account information. Furthermore, to prevent fraudulent authorization requests from being sent to the cardholder, the data could be encrypted, and signed by the private key of the credit provider. The cell phone would have the public key of the credit provider and be able to confirm that the information came from the credit provider (this type of technique is standard in secure websites today).

This technology is designed to greatly reduce the occurrence of credit card fraud while giving card holders control over what is being purchased in their name.

