Apparel™

Protect Mobile In-Store Payments From Relay Attacks

— December 09, 2014

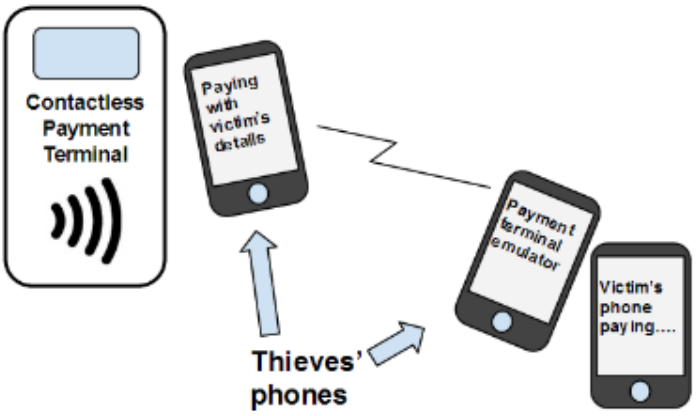
One of the hot mobile technologies these days is mobile in-store payments. The idea is simple and appealing -- instead of carrying around credit cards, customers can pay in a store by simply holding their smartphones near payment terminals.

Mobile payments got a huge boost in the United States with September's launch of **Apple Pay**. While mobile payments have been growing steadily in the past year, Apple's announcement is likely to legitimize the use of smartphones for in-store payments, especially in the United States. Mobile payments have already gained broad adoption in many areas of Africa and Asia, and are spreading in Europe.

The major players include consortiums such as **SoftCard** and **MCX**, financial powerhouses such as **Visa and MasterCard**, as well as technology vendors such as **Google Wallet** and **PayPal**.

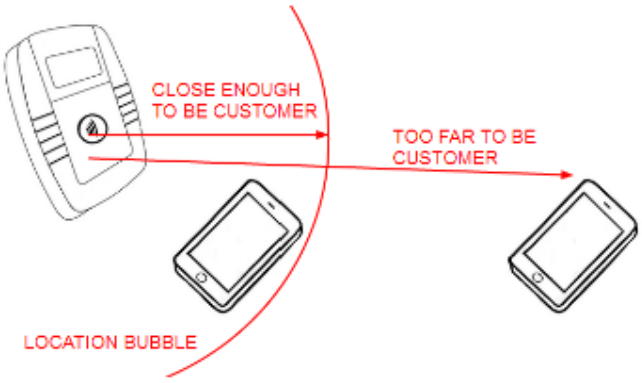
Most mobile in-store payment solutions are based on near-field communication (NFC) technology. NFC communicates over very short distances, such as the distance between a payment terminal and a cellphone that a customer is swiping. NFC supports encrypted communication, so that nearby devices cannot eavesdrop. The short distance of NFC communication is considered a benefit for this purpose, since it reduces drastically the odds that an eavesdropping device can be within range without being seen.

As this new technology reaches market, however, new security concerns have emerged. NFC payments can be vulnerable to what's called a "relay attack." Simply put, in a relay attack, if someone can get access to your mobile phone (or your credit card with contactless chip inside), they can use their own phone to impersonate a store's payment system, and pass your phone's payment details to a partner's phone, located in a real store, to make the purchase using your payment details. With two phones acting together to relay the communication, the store's payment system and your phone think that they're communicating securely. This would only require a minute or so of access to your phone.



Relay threats are one of the challenges being addressed by the eGo Project, an initiative by Gemalto to develop next-generation electronic payment and transaction solutions. One of the methods used by eGo to solve this vulnerability is what's called location bubbles. In Gemalto's approach, the device making the payment and the point-of-sale terminal ensure that they are within a short distance of each other, such as one or two meters. This requires that the customer's mobile phone is able to measure its indoor location accurately, either measuring the precise distance to the POS terminal or comparing its precise location to that of the POS terminal. This location data is communicated with encryption to avoid a relay attacker modifying the location data en route.

Precise distance and location measurements are provided in the eGo Project using ultra-wideband (UWB) technology implemented on a chip. This UWB chip is designed specifically to measure distances and locations very accurately, to within 10cm. At the same time, UWB provides secure wireless communication with higher bandwidth than Bluetooth.



UWB radio is designed to deliver more accurate location and distance measurements in the presence of interference and multi-path issues. When narrowband radio signals (including most wireless systems on the market today) go through or around obstructions, they are received at the other end multiple times, and effectively cancel each other out, affecting the accuracy of the measured distance. But UWB signals transmit much shorter and sharper pulses, and remain distinct even where there are obstructions and multiple paths of transmission. In addition, UWB systems measure location based on the time of flight of the signals, and not based on the signal strength, which is more affected by people's bodies and other interference. Most other radio-based location systems on the market are based on received signal strength measurements.

As mobile in-store payments gain acceptance, the market will demand stronger security precautions, especially given risks such as NFC relay attacks. Location bubbles based on precise distance and location measurements, as are used by the eGo Project, will be a key method for keeping mobile in-store payments secure.

*Luc Darmon is vice president of business development for **DecaWave**, whose recently launched UWB chip is a single-chip transceiver designed to be embedded in small electronic devices. This is critical for the eGo Project, which requires that its systems have very low power requirements and very small sizes.*