itbusiness.ca
Business Advantage through Technology

Print

Google Wallet and NFC security: guarding against 'sharks with lasers'

Security researchers are exploring ways NFC-enabled mobile payment systems like Google Wallet could expose users to hackers looking to scoop payment information, and other security risks. Meanwhile, a Google engineer promises the NFC security is 'designed to be safe from even sharks with lasers.'
9/29/2011 6:01:00 AM
by Brian Jackson

The emergence of mobile payments may offer another convenient way to pay, but does it also open up a door for hackers to pick your pocket?

This month, the first field trial of using smartphones to pay at the cash went live in San Francisco. Using the near field communications (NFC) chip technology in Samsung's Nexus S and the newly-released Google Wallet app, smartphone users could pay at the cash registers already outfitted MasterCard's PayPass readers. Other Android-based devices also pack an NFC chip, and it's even rumoured to be in Apple's soon-to-be unveiled iPhone.

Adding payment functionality to smartphones makes sense – users carry them everywhere, replacing personal organizers, digital cameras, and phone books with the digital multi-tools, so use as an alternative to payment cards in some situations is not a big leap. But it also raises new security questions as device owners entrust their payment information to a new technology, and allow it reside on a device that could easily be lost or stolen.

There's no need to stress, says Rob von Behren, a software engineer with Google Inc., specifically working on the Google Wallet team. "It's designed to be safe from even sharks with lasers."

Express IT | Mobile payments will be best cash alternative

Key to the security of the payment information in the Nexus S is its storage separate from the normal phone memory in a digital vault dubbed the Secure Element, designed to act as a one-way door for payment information that restricts access. This is the same chip found on plastic payment cards that allow touch payment such as Visa's PayWave. But there's several layers of security protection on top of it.

"The hardware in the chips prevent things like scanning the memory of the device," von Behren says. It's loaded with heat, light, and voltage sensors to detect any hacker tricks attempting to circumvent the chip's normal behaviour. "When those are detected and the chip goes into lockdown mode and blows a fuse internally so it can't be used again."

Security analysts at New York-based Intrepidus Group who've been "fuzzing" Google Wallet since its release wonder if some of the same attacks seen on Nokia phones with NFC chips in Asia could migrate to the Android platform. Since "rooting" or replacing the manufacturer-issued operating system on an Android device is common, principal consultant Corey Benninger wonders if that could open up more risk to the Nexus S Secure Element.

"Any time you root your Android device, you're taking the risk that other applications could elevate their privileges and gain additional access," he says. Intrepidus will be presenting about NFC security at Toronto's upcoming Sector conference, Oct. 18 and 19.

But that's not a concern, according to von Behren. While the Secure Element is on the same physical die as the actual NFC chip that transmits user data, it is logically separate and independent, he explains. There is actually no mechanism on the phone to allow other applications to read information from the chip. It needs to be prompted by interaction with an NFC tag, like those found at payment locations.

Benninger also worries that a battery-powered NFC chip could be read at a further distance away by an unauthorized reader. Such reader devices can be purchased for a nominal price on the Web, he says, and be

pointed with malicious intent at unsuspecting smartphone users. Normally NFC chips can only be read from a few inches distance, but those chips are on plastic cards without a power source.

Those chips are powered by the readers, says Intrepidus security consultant Max Sobell, and once that pairing occurs it is possible to pick up a reading from further away.

On plastic cards, “once the chip wakes up, it can actually keep state based on the power this wave is sending it,” he explains. “It will modulate the wave and reflect that energy back, and that's how the transaction will take place.”

The type of radio communication used for NFC means it is difficult to get a reading from a distance, von Behren retorts. “You get a huge amount of interference on those frequencies.”

Related Story | Mobile payments offer big benefits

To be activated, the Nexus S must be powered up and the user's Wallet PIN must have been entered. So the chip won't be powered up when the phone screen is off.

As NFC chips become standard hardware on more smartphones, developers will look to use the technology for purposes beyond mobile payments. That could open up a whole other can of worms when it comes to security, the Intrepidus analysts say. In one early example of such an exploit, an NFC tag-reading application could be made to request more memory use than was available on the device, crashing the application.

More serious concerns include user privacy, Benninger says. “Some tags will have unique IDs that could be used to track a person's device… By storing too much information you could be compromising your user's privacy.”

More low-level attacks could be undertaken by simply swapping publicly-posted NFC tags with different ones created by hackers. An unsuspecting user could swipe their smartphone expecting one action, and unwittingly trigger a different one.

For example, swapping the tags found on vending machines could see thirsty consumers swiping their phone with the intent to buy a soft drink, but they are actually paying for a chocolate bar on another nearby machine. Or a hacker could design an NFC tag that would direct a phone to a URL containing malware.

That's a possible attack vector, von Behren says.

“The same kind of thing happens all the time with e-mail, with whatever the phishing attack du jour is,” he says. “This is another way you could trick people to go to the phishing site.”

To defend against such attacks, developers could make use of the cryptographic features built into the NFC Data Exchange Format (NDEF) used to transfer information from tags to NFC chips on phones. A signature can be stored on the tags that would have to match an application on the phone, authenticating that tag.

“The framework is there, but the implementation is in the weeds for a lot of developers at this point,” Benninger says. For now, data transferred from tags “needs to be seen as untrusted data coming into your application. The same way you validate Web data, you'll need to do the same with NFC tags.”

For businesses interested in preparing to accept mobile payments, Google offers advice on its Wallet Web site. It's not yet clear when Google Wallet will be available in Canada.

Brian Jackson is the Associate Editor at ITBusiness.ca. Follow him on Twitter, read his blog, and check out the IT Business Facebook Page.

Print

Close Window