pipeline
global security

June 30, 2011

INTERVIEW: Hold the Google phone! Is NFC actually secure?

by Hollie Slade

Investors are falling over themselves to invest in mobile payments. Just today Square, the mobile payments startup from Twitter creator Jack Dorsey closed a $100 million Series C propelling the company to a valuation of over $1 billion. Juniper Networks, a transaction security provider staked the claim that near field communication (NFC) technology will soon overtake credit card transactions as the number one form of payment and be worth $50 billion in 2014. Google partnered with MasterCard, Citigroup and Sprint to launch the Google Wallet, which utilises NFC technologies. The NFC hype train is amped up and attracting big bucks.

However, a pertinent question remains. Is the technology actually secure? Kenneth Weiss, inventor of the SecurID tokens, whose technology is relied upon by more than 100 million people, Fortune 500 companies, as well as corporations, consumers, governments, and banks in more than 30 countries, told Global Security pipeline in an exclusive interview that he doesn't think so.

It is worth pointing out that Weiss was founder, Chairman and CTO of Security Dynamics, now RSA, when the company went public in 1994, but he left in 1996, 10 years before the EMC acquisition and well before RSA's recent corporate security breach. The SecurID technology is still used in the world's top-secret computers today.

Weiss' company, Universal Secure Registry LLC (USR), is an enabling mobile payment security technology and identity authentication system. Weiss maintains that the USR electronic wallet is the only mobile transaction technology that does not transmit sensitive information from or store exploitable information in the mobile device.

Unlike other electronic payment technologies being tested or introduced by companies such as Google and Isis, private or sensitive information is not stored on the mobile device or transmitted at the point of sale (POS) with USR. The USR electronic wallet provides a convenient and reliable way to authenticate identity with three factors quickly. This enabling technology acts as a trusted agent for personal transactions including mobile payments, financial transactions, tolls, vending machines, computer/network/cloud access, physical access, licenses and all privileges associated with identity.

“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.

“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,” says Weiss.

Weiss has decided that now is the time to license the technology – including the algorithms, designs, and software. The components of the technology do not need to be tested because they are well established and already in use; Weiss has simply strengthened the algorithm and reconceptualized how the technology can be implemented.

The versatility of the technology is the most important element as it means that it is a much more secure means of providing access control to homes, computers and financial transactions.

The company has been in stealth mode until the critical mass of all relevant patents and proprietary components have been finalized, which occurred in the last year.

Weiss is uncompromising on NFC when used to radiate exploitable or private information: “I can read your credit card remotely while it’s in your pocket with near field communication, I can certainly read it at the point of sale surreptitiously if I have a receiver in my briefcase or around my body. All they are doing is radiating very private information that is now easier to counterfeit. If I’m a hacker and I get those codes, I can be you for as long as it takes for them to shutdown that particular credit card.”

Weiss said that the company is prepared to implement the technology themselves, but that the wiser choice is not to add noise to the already chaotic market, making him circumspect on raising capital.

“If we chose to raise money and go forward, which we are certainly prepared to do, there would be a long acceptance curve and we’d add some additional chaos to the market; if USR technology is implemented by mobile phone carriers, or the major credit card companies, there’s a very short hockey stick curve of acceptance, and we’ll all be better protected,” Weiss said.

For more information on Universal Secure Registry please contact Kenneth Weiss, CEO on KPW@usrid.net

###

http://www.globalsecuritypipeline.com/Main.aspx#intel&id=7156