The Apple Pay approach to mobile payment turns the security conundrum upside down by keeping data out of thief-magnet servers

By Evan Schuman

Follow

Computerworld | Sep 23, 2014 2:00 AM PT

- Apple

Security is not always about creating a stronger deadbolt or a more protective firewall. Sometimes it's about understanding what motivates potential attackers and using that knowledge to make your valuables look less attractive, either directly or by comparison. It's this more sophisticated approach that Apple is using with its newest devices and software.

- Evan Schuman: Google eyes the preteen setEvan Schuman: Barnes & Noble plays into Amazon's handsEvan Schuman: Supreme Court on obvious patents: Common sense isn't so horribleEvan Schuman: The data dangers of free public Wi-FiEvan Schuman: Do you know the people you're following on Twitter? Neither does Twitter, apparentlyEvan Schuman: Is Google forgetting that interactivity pays its bills?Evan Schuman: What if you can't trust your inbox?Apple's mobile payment rolling out despite problemsApple outsmarts the thieves SEE MOREIf you wanted to secure a house, these psychological tactics might include leaving an old wreck of a car in the driveway, which would suggest that there's little of value to be found in the house. Or you might volunteer to help spruce up your neighbor's house, making it look like a more profitable theft target than yours. (Hey, I didn't say that these were necessarily *ethical* examples.)

  More like this

iPhone 6 and iPhone 6 Plus review: Bigger is in fact better (in the right...

- 

  5 cybersecurity tips for consumers: Lessons learned in the enterprise

- Fingerprint Faceoff: Apple Touch ID vs. Samsung Finger Scanner

In enterprise IT, the idea is the same. Protecting your content against a brute-force attack is essential, but doing what you can to make thieves look elsewhere is potentially an even better strategy. When Apple introduced Apple Pay this month, it demonstrated an understanding of both tactics.

Apple Pay does something that turns the security conundrum upside down. The problem has been that enterprises, as self-centered profit seekers, are uninterested in spending a lot of money to improve security for all or to shut down gangs of cyberthieves. All they want to do is make the thieves stop attacking them. If Apple Pay and other payment systems using the same model become widely adopted, that would become less of an issue, because enterprises would look like less appealing targets. (More on this later.)

Something else that Apple did, perhaps only as a way to improve usability, also boosts security. With every earlier NFC payment app, the shopper had to start the process by launching that app. To speed things along, Apple bypassed that step and allowed Apple Pay to do its magic solely by proximity to the signal and by the shopper putting a finger on the phone's biometric scanner. That is certainly faster and easier, but that fingerprint scan is also more secure than the traditional use of a signature or a PIN. Yes, I know that the fingerprint reader is full of security holes — there are various methods for copying a fingerprint from a stolen phone and using it to trick the scanner into authenticating incorrectly — but despite that, it is an order of magnitude more secure than signature and PIN. (It should be noted that Apple has paid attention to the criticism. The latest version of its biometric scan makes better use of methods for detecting live tissue.)

Let's not attack Apple's fingerprint scanner for being less than perfectly secure when signatures offer pretty much zero protection, and PIN has plenty of problems of its own.

Comment [A1]: Apple Pay uses Near Field communication (NFC) and Fingerprint Recognition (FR) coupled with limited content exchange (only payments and coupons etc) can be exchanged and traded. NFC guarantees delivery of the transaction to the Point of Sale (POS) device and Apple guarantees delivery of the message to the destination.

Apple Pay content is limited in scope (context) and the security measures used (NFC, FR) allows them to do away with elaborate payment authentication (who?) and authorization (privileges?).

But why concoct elaborate security schemes when payment should be enabled between any two people given proper encryption? For example, email encryption can be set up today using Outlook between any two people. It even works with an Outlook client in gmail. Email is not guaranteed delivery which is what Apple Pay is adding to the mix. My point is, I could concoct a payment system today using only Outlook with encruption. Apple is making electronic payment as ubiquitous and the Apple iPhone which is considerable (yet).

Hiveware operates using **synchronous informed consent**. Hiveware operates like natural language where each word is also a kind of generalized informed consent among participants of a particular language group. Because we users all have copies of concepts in our brains and we ahead of time have agreed to learn (childhood) them and learn new ones as an adult, we have the ability to understand and communicate with each other. Hiveware is conceptually built to emulate this natural language process. Delineating the context of which we are giving or receiving consent about is difficult. That is why new apps have to limit their context to obviousness (eg, Apple **Pay** (not money), Twitter (one short sentence per person),)

Cashiers are hardly experts in handwriting recognition, and in any case it's been decades since retailers urged them to compare signatures with the one on the card. And most PIN deployments in the U.S. — including Apple's default — are four digits, which is woefully inadequate. It is quite weak for online usage, given the relative ease of cracking a four-digit code, and it's far from foolproof in-store, where the criminal technique of shoulder surfing is common — the thief just looks over someone's shoulder and learns the PIN by watching it get entered.

So I have to give a thumb up to fingerprint scanning. But even better is that Apple is storing payment-card data in the iPhone's Secure Element, which is simply a chip in the phone. It shouldn't be very easy to access and, even if that happens, it's simply a token that leads to encrypted data. But here's the really good part: The payment data is not stored on Apple servers or held by the retailer. This is how Apple eliminates the problem of profit-oriented retailers not working together to stop data breaches. When retailers are no longer in possession of payment data, they cease being the target.

What Readers Like

- 

Naked celebs: Hackers download sext selfies from iCloud

- 

iOS 8 problems not so magical: Slow, Laggy, Bloaty, Crashy, Buggy, Drainy and...

- 

How to decide which iPhone 6 is right for you

Ah, *when* that happens; there's the rub. Apple Pay is showing the way out of some sticky security problems, but its debut (probably by the end of October) doesn't eliminate the problem. I'd calculate that this coming holiday season, 99.999% of all merchant transactions won't use Apple Pay. It's going to be a very long time before that figure gets whittled down significantly.

It will help if other mobile-payment players see the wisdom of this approach and emulate it. When enough payments are made this way, so that card data stored is on personal devices and not conglomerated on big enterprise server systems, ROI goes out the window for cyberthieves. They need to access huge numbers of cards, ideally tens of millions or better. That's because cards age out quickly, and once a breach is discovered, that aging-out is greatly accelerated. Cyberthieves are not going to see much percentage in hacking tens of millions of phones to get that kind of data quantity.

I know that the mass collection of payment card data won't be eliminated by the Apple Pay model, even if it's a huge success. Card issuers are still going to retain those sorts of records. But in general, financial operations have better security than retailers, and they also have more incentive to promote better security for all.

Comment [A2]: An why not? Synchronous Interactive informed consent has that potential. Bitcoin can transfer context-less number-of-units (aka, money) because it has figured out using pure computer science how to ensure that there is one and only one transaction between two people. Add computerized context to what Bitcoin does and you have Hiveware.

You've gotta give credit to Apple. It didn't just use a better deadbolt. It outthought the thief by better understanding him.

Evan Schuman *has covered IT issues for a lot longer than he'll ever admit. The founding editor of retail technology site StorefrontBacktalk, he's been a columnist for CBSNews.com,* RetailWeek *and* eWeek*. Evan can be reached at eschuman@thecontentfirm.com and he can be followed at twitter.com/eschuman. Look for his column every other Tuesday.*