First Data's composite security system - a game changer?

Processing giant First Data Corp. recently launched a pilot security program to guard merchant POS systems, and the company hopes it will become a benchmark in the fight against data theft.

The pilot program, which will be tried on about 400 merchants over the next four months, uses a multipronged security architecture that combines "asymmetric" encryption with tokenization. The program was developed through a partnership with EMC Corp., which owns the RSA SafeProxy architecture First Data is deploying. Under the First Data program, the security architecture has been rebranded TransArmorSM.

According to Craig Tieken, Vice President of Product at First Data, the program will run through July 2010; the company plans to launch the product publically thereafter. He said the goal is to have around 100,000 merchants linked to the TransArmor system by the end of 2010. He added that it is aimed at merchants of all sizes.

"You're starting to see increased sophistication of cyber crime that's no longer just targeted at the big guys; it's moving down market," Tieken said.

"So as big guys harden up their systems, [cyber criminals] are going down low, and our market research shows that although there's quite a bit of education to be done with the merchant community, awareness is growing rapidly."

For merchants with modern terminals, the product can be implemented with a simple computer download, Tieken said. He noted that its implementation would both fortify merchant environments and, through tokenization, dramatically simplify the Payment Card Industry (PCI) Data Security Standard (DSS) compliance process by relieving merchants of sensitive data storage.

"There's the part of your system capturing card data and then encrypting it; that's what's left within the scope of your PCI [compliance burden]," he said. "The rest of it is no longer touching card data. When I'm not storing card data at all and I'm encrypting card data when it's in motion ... it becomes much easier to answer those [PCI] questions, and a lot can be prepopulated as a standard response."

Extra-strong encryption

According to Tieken, TransArmor's front-end is strengthened beyond standard encryption schemes through a divided, asymmetric encryption method. Data is encrypted within the merchant's terminal but can only be decrypted by First Data at the processing end. Thus, thieves who penetrate a merchant's POS system theoretically have no way to view the raw data therein. Even if they crack the encryption scheme, they can't use that formula for decryption.

"It's a method of doing encryption in which you have a key pair that's split apart," Tieken said. "The public key is given to the merchant. That's the component that does the encryption at the merchant location but can't decrypt. So they send [First Data] this encrypted block of data, and we have the corresponding second key in our data center. So even if someone got a hold of the key from the merchant they can't do anything with it."

Tieken added that encrypted payment data is decrypted by First Data and returned to the merchant in the form of a token – a random set of numbers that allows the merchant to conduct chargebacks, recurring billing and other post-transaction functions without handling sensitive card data. The token retains the last four digits of the original card number so that customers can identify their cards on receipts.

Extra security layer with recurring billing

Furthermore, under the TransArmor solution, a consumer using recurring billing is represented by a unique identification number separate from the token returned to the merchant. If continuous payments were made with the original token, Tieken said, a stolen token could be used just like a credit card number in a recurring billing scenario.

"In the card-not-present recurring base, what we have is a class of the token that actually represents me and the biller to First Data differently than the token that is sent back for purposes of [merchant] reporting and getting paid," he said. "So I actually have a consumer ID that represents me to [for example] my electric company for purposes of recurring billing."
"If I just took my financial token used for reporting and chargeback exception items and said, 'Take that token and submit a new transaction,' then I can start to launder those things, and I've done nothing but replace one card number with another card number."

**Major step forward**

Theodore Svoronos, Certified E-Commerce Consultant with Group ISO Inc., said First Data's program marks a significant step forward in the payment business's longstanding fraud fight. The technology being used isn't anything new, but the deployment of a composite token/encryption security product on the scale intended by First Data would be groundbreaking, he said.

"All these security products have been around since 2000, 2001 – all these bits and pieces," Svoronos said. "The problem we've been having in this industry is the attrition rate, the low adoption rate, customer drop off and sales going down because [merchants] don't get it. ... By First Data adopting this, they are becoming a leader in this space. They have the wherewithal and financials and ability to do it, and they can cherry pick the best of the best and put it together, and RSA is phenomenal.

"PCI is a wonderful situation and well-needed, but to some point it's still reactionary. I believe in a proactive approach, and this approach First Data is trying is a proactive approach.

And those [merchants] that do decide to jump on board this train before it leaves the station will realize the value down the road."