InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Credit Card Processors Getting Encryption Religion

Top providers are touting new services. Yet many businesses that accept credit cards aren't ready for end-to-end encryption.

By Thomas Claburn, InformationWeek
Nov. 21, 2009
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=221900322

Steven Elefant, CIO of Heartland Payment Systems, doesn't believe in software security. "There is no such thing as totally secure software anymore, and there probably never will be," he says.

Elefant comes by his realism the hard way, having seen first-hand the lengths to which cybercriminals will go to gain access to valuable financial data. He joined Heartland Payment Systems, one of the largest payment processing companies in the United States, in January, the month the company reported that its payment processing network had been compromised for several months by data-stealing malware.

Although the exact number of records affected by the breach remains undisclosed, Heartland's handling of more than 100 million transactions per month for more than 250,000 businesses almost guarantees that the breach is among the largest in history.

Heartland lost about $500 million, or more than three-quarters, off its market capitalization following the breach. Having gained that back, Heartland is on a mission to get security right. And encryption is at the heart of that effort.

The company's plan involves using a combination of software and hardware to implement end-to-end encryption, which aims to protect payment data across five possible zones of transit--from the merchant's credit card terminal, across the payment processor authorization network, through the central processing unit or host security module, inside a direct access storage device or archival storage, and over to card-issuer authorization and settlement systems.

The idea of protecting card data from cradle to grave may sound obvious, given its value and the criminal efforts to steal it. But the payment processing industry has focused on communication more than security, Elefant says. "The industry was set up to be connected," he says. "The brands have done a really good job connecting everybody."

The focus now has shifted to security, since it's becoming clear the old approaches aren't enough. "The criminals have been breaking into data in transit, and none of the controls have been working properly," says Gartner Research VP Avivah Litan.

End-to-end encryption has been avoided for years in large part because of the high cost. The payment infrastructure is a mix of new equipment and decades-old hardware that can't handle the complex cryptographic technology that's now available, says Craig Tieken, VP of merchant product management for the largest U.S.

payment processor, First Data. "Forcing a merchant to rip and replace hardware often ends the conversation right there," he says.

What's more, the card brands, such as Visa and MasterCard, haven't wanted to mandate end-to-end encryption. PCI, the industry group created by card issuers, set security standards that require encryption for data in transit over public networks, but not over private networks and not between retailers and other companies in the payment chain, including payment processors and card issuers. Changing to end-to-end encryption of data in transit over private networks among retailers, processors, and issuers "really requires a sea change in infrastructure," says Litan.

But the breach of retailer TJX in 2006 and the Heartland breach last year have focused the industry on end-to-end encryption. The TJX case involved the theft of more than 45 million credit and debit card numbers from its IT systems, leading to TJX absorbing a $118 million charge in 2007 for the costs of the massive security breach. It was later learned that one international criminal group had led some of the most publicized credit card hacks, including TJX. The U.S. ringleader, Alberto Gonzalez, pleaded guilty this September to 20 federal felonies.

Encryption Looks Like Smart Business

For Heartland, embracing the technology is a way to turn its victimization into a market opportunity. Heartland, says Litan, "has been trying to prove to their customers and the rest of the world that they are serious about security and the rest of the processors have become more competitive with them."

For Verifone, which makes payment terminals, the competition has taken the form of patent litigation. The company claims that Heartland's forthcoming hardened E3 payment terminal infringes on a 2005 patent it holds. Heartland responded with a countersuit and recently accused Verifone of "false claims and unethical attempts to scare our customers."

The competition can also be seen in the new partnership between First Data and EMC's RSA Security. In September, the two companies announced that they're partnering to deliver a service called First Data Secure Transaction Management, which will provide end-to-end encryption with tokenization. That process replaces sensitive card data with a token reference number that merchants can store with confidence, because the token has no value to thieves. "It's important that the merchant is able to securely transmit the data upstream, but post-authorization, there's not really a need to hold card data in their environment," says Rob McMillon, RSA's director of solution development.

Tokenization lets merchants run analytics on sales data without the risk of storing usable payment card numbers. While this makes merchants more dependent on the vendor providing the payment security technology, Tieken says First Data's contract with merchants can stipulate that First Data provide detokenized data to let merchants take their business elsewhere, if desired.

End-to-end encryption "is long overdue," says McMillon. "All of the major processors are either offering their solution or in the process of rolling one out."

So can we all soon rest easy, knowing crooks can't crack this code? Many retailers and others that accept credit cards might not find encryption that enticing. "It's costly, and it's not foolproof," says Litan. She cites the case of a retailer that implemented end-to-end encryption only to have an auditor defeat the system by finding the encryption keys unprotected. She also describes how a major retailer had put encryption in place but couldn't demonstrate the ROI.

Encrypted data isn't invulnerable. The recent indictment of four men for hacking into RBS WorldPay last year noted that two defendants developed a method by which the conspirators reverse engineered personal identification numbers from the encrypted data on the RBS WorldPay computer network.
Litan, however, is skeptical that the encryption itself was cracked and suggested a more likely scenario was that the encryption had been defeated after the conspirators found a way to grant themselves super-user privileges inside RBS WorldPay's Hardware Security Module.

Litan says that while the payment processing companies are pushing for greater security, the card brands have yet to agree on a standard that works throughout the payment chain. There's not really a sense of urgency--except among the card processors, which sense a chance for competitive differentiation.

--Thomas Claburn *(tclaburn@techweb.com)*