



BOB CARR is chairman and CEO of Heartland Payment Systems. You can reach him at bob.carr@e-hps.com.

Anatomy, Aftermath of Criminal Breach, Part 2

In the first article of this series I discussed several of the widely held beliefs in our industry that I believe are wrong-headed and harmful to the almost 150,000 convenience store operations in our country. In this article I would like to focus on current and future enhancements to payments security that will begin to ease the pain of costly PCI compliance and losses that unattended fueling operations suffer from counterfeit card fraud.

The discussion around the July 1, 2010, deadline to upgrade all unattended fueling PIN devices to Triple-DES (TDES) devices provides a perfect forum to explain the value of encrypting tamper-resistant security modules (TRSMs) and the differences between encryption and tokenization techniques that are being talked about at length in the industry today. The differences are a bit technical but I think they are crucial for our industry, and I will explain them as accurately and as simply as possible.

I believe the vast majority of c-store operators don't know the primary rationale for the forced upgrade to TDES. In fact, I think the majority of people in the payments industry don't understand the real reasons, either. I have heard from many in both the petroleum and the payments industries that TDES is being required because lesser forms of encryption have been compromised by the criminals. That is a common belief, but it is not correct.

The reason is that back in the mid-



'80s, the designers of PIN encryption for many pump controllers were not thinking ahead or were oblivious to potential security issues such as hardware skimmers. C-store operators have been paying the price for this lack of forethought for many years. What was the mistake?

HOW A TRSM WORKS

Are you old enough to remember when you could first go to a machine called an ATM and get real American dollars by inserting your card and keying in your four-digit PIN? That was as far back as the 1970s, and the ATM PIN system has worked very well for decades—no major problems with the technology. In fact, this technology worked so well that retailers began to

purchase PIN pads and accept PIN debit transactions in their stores. That began in the 1980s, gained steam into the '90s and '00s and continues its momentum today.

So what is different for fuel pumps? What is the difference between the ATM technology of the '70s, the retail PIN pads of the '80s and the fuel-pump technology of today and yesterday? The answer is TRSMs. The ATM and the retail store PIN pad have always come with a TRSM with encryption technology embedded into the hardware—all attached to the PIN pad into which you key your four-digit PIN. (Admittedly, some of the original ATMs used a PC inside the ATM instead of a TRSM; unlike with unattended fueling, this deficiency was quickly remedied.)

What does a TRSM do? It converts the analog data coming off the magnetic stripe into digital gibberish (aka encrypted PINs) before it gets onto the electronic transmission lines that transport the electronic payment data to the computer that sends the transaction to the payment processor. To be perfectly accurate, there is a very short wire that connects most of the TRSMs to the read heads. For this short distance, typically an inch or two, the PIN is in the clear (meaning it has not yet been encrypted). That very short wire is typically within a hardened device secured with highly effective, tamper-resistant materials.

All ATMs in the world and all retail PIN pads have TRSM devices embedded adjacent to the card reader heads,

and are connected by this very short wire that is protected inside of a hardened device. I am not aware of skim-

In war, it is **best to be very close to your bunker** when attacked. The same is true for PINs that are subject to attack by skimmers.

ming devices being successfully inserted on these wires or software ever compromising a TRSM with software skimming devices. If these attacks have succeeded over the past 30 years, they have been uncommon and are not well

known in the payments community.

WHERE THE DANGER LIES

Now we come to the unattended fuel device. The CRIND (card reader in the dispenser) contains the read heads at the pump. Where is the TRSM for many of the older devices that are not up to the TDES standard? It doesn't exist! There is no TRSM in many CRINDs.

In these cases the PIN is encrypted by software in the computer (aka the pump controller), typically inside the store—usually far, far away from the CRIND. The transmission lines from the CRIND to the pump controller are long. These transmission lines are not encased in a hardened device. In short, they are not protected from skimming devices at all. Who made the “business decision” to save a few bucks in the short run? Today TRSM devices cost less than \$25 to manufacture. Back in the mid-'80s, design engineers were not thinking about skimmers, but one would think that a solution to this problem could have come sooner and therefore with less expense. But so much for 20-20 hindsight!

In war, it is best to be very close to your bunker when attacked. The same is true for PINs that are subject to attack by skimmers. To send a PIN in the clear from the CRIND all of the way along the path to the computer inside the store is not good. But that is how some pre-TDES CRIND and pump controllers were designed.

Transmission of PINs in the clear from the read heads to a computer is dangerous with unattended fuel pumps. We know of many, many cases of physical skimmers being inserted on these transmission lines at c-stores



across America. The result is that track data, including PINs in the clear, is being captured by the criminals and used by criminals to rack up fraudulent charges at stores and to drain bank accounts.

FIND YOUR BUNKER

That brings us to a comparison of encryption with tokenization. To convert a card number from analog data to digital gibberish requires an encryption engine or a tokenization engine. (I will cover these techniques in more depth in the next article in this series.) The question is, when is the data in the clear before it gets encrypted or tokenized by the engine? For an ATM, the engine is inside the TRSM. For a retail store, the engine is inside the TRSM. For a fuel pump, the engine may be at the CRIND, but it could also be inside the store in the pump controller—unless the operator elects to implement TDES. TDES comes with a TRSM. Where is your bunker?

By definition, tokenization takes place in the tokenization engine, which is typically located in the computer system of the gateway of the tokenizing company or the computer of the payment processor. How does the card number get to the tokenization engine? If there is no encrypting TRSM, the card number is transmitted in the clear.

Cybercriminals are experts at inserting sniffers (software skimming devices) onto gateways and into processor networks to intercept card numbers in the clear. This is what happened to Heartland, Hannaford Brothers and hundreds of other merchants and processors. Without a TRSM immediately converting the analog magnetic stripe data into gibberish, the exposure to cybercriminals exists in spades.

In the next article of this series I will discuss the coming wave of new enhanced security techniques and what that might mean for the c-store industry in the next few years. ■