PIN Crackers Nab Holy Grail of Bank Card Security

By Kim Zetter April 14, 2009 | 10:55:00 PM Categories: Crime

Hackers have crossed into new frontiers by devising sophisticated ways to steal large amounts of personal identification numbers, or PINs, protecting credit and debit cards, says an investigator. The attacks involve both unencrypted PINs and encrypted PINs that attackers have found a way to crack, according to an investigator behind a new report looking at the data breaches.

The attacks, says Bryan Sartin, director of investigative response for Verizon Business, are behind some of the millions of dollars in fraudulent ATM withdrawals that have occurred around the United States.

"We're seeing entirely new attacks that a year ago were thought to be only academically possible," says Sartin. Verizon Business released a report Wednesday that examines trends in security breaches. "What we see now is people going right to the source ... and stealing the encrypted PIN blocks and using complex ways to un-encrypt the PIN blocks."

The revelation is an indictment of one of the backbone security measures of U.S. consumer banking: PIN codes. In years past, attackers were forced to obtain PINs piecemeal through phishing attacks, or the use of skimmers and cameras installed on ATM and gas station card readers. Barring these techniques, it was believed that once a PIN was typed on a keypad and encrypted, it would traverse bank processing networks with complete safety, until it was decrypted and authenticated by a financial institution on the other side.

But the new PIN-hacking techniques belie this theory, and threaten to destabilize the banking-system

transaction process.

Information about the theft of encrypted PINs first surfaced in an indictment last year against 11 alleged hackers accused of stealing some 40 million debit and credit card details from TJ Maxx and other U.S. retail networks. The affidavit, which accused Albert "Cumbajohnny" Gonzalez of leading the carding ring, indicated that the thieves had stolen "PIN blocks associated with millions of debit cards" and obtained "technical assistance from criminal associates in decrypting encrypted PIN numbers."

But until now, no one had confirmed that thieves were actively cracking PIN encryption.

Sartin, whose division at Verizon conducts forensic investigations for companies that experience data breaches, wouldn't identify the institutions that were hit or indicate exactly how much stolen money was being attributed to the attacks, but according to the 2009 Data Breach Investigations report, the hacks have resulted in "more targeted, cutting-edge, complex, and clever cybercrime attacks than seen in previous years."

"While statistically not a large percentage of our overall caseload in 2008, attacks against PIN information represent individual data-theft cases having the largest aggregate exposure in terms of unique records," says the report. "In other words, PIN-based attacks and many of the very large compromises from the past year go hand in hand."

Although there are ways to mitigate the attacks, experts say the problem can only really be resolved if the financial industry overhauls the entire payment processing system.

"You really have to start right from the beginning," says Graham Steel, a research fellow at the French National Institute for Research in Computer Science and Control who wrote about one solution to mitigate some of the attacks. "But then you make changes that aren't backwards-compatible."

PIN hacks hit consumers particularly hard, because they allow thieves to withdraw cash directly from the consumer's checking, savings or brokerage account, Sartin says. Unlike fraudulent credit card charges, which generally carry zero liability for the consumer, fraudulent cash withdrawals that involve a customer's PIN can be more difficult to resolve since, in the absence of evidence of a breach, the burden is placed on the customer to prove that he or she didn't make the withdrawal.

Some of the attacks involve grabbing unencrypted PINs, while they sit in memory on bank systems during the authorization process. But the most sophisticated attacks involve encrypted PINs.

Sartin says the latter attacks involve a device called a hardware security module (HSM), a security appliance that sits on bank networks and on switches through which PIN numbers pass on their way from an ATM or retail cash register to the card issuer. The module is a tamper-resistant device that provides a secure environment for certain functions, such as encryption and decryption, to occur.

According to the payment-card industry, or PCI, standards for credit card transaction security, PIN numbers are supposed to be encrypted in transit, which should theoretically protect them if someone intercepts the data. The problem, however, is that a PIN must pass through multiple HSMs across multiple bank networks en route to the customer's bank. These HSMs are configured and managed differently, some by contractors not directly related to the bank. At every switching point, the PIN must be decrypted, then re-encrypted with the proper key for the next leg in its journey, which is itself encrypted under a master key that is generally stored in the module or in the module's application programming interface, or API.

"Essentially, the thief tricks the HSM into providing the encryption key," says Sartin. "This is possible due to poor configuration of the HSM or vulnerabilities created from having bloated functions on the device."

Sartin says HSMs need to be able to serve many types of customers in many countries where processing standards may be different from the U.S. As a result, the devices come with enabled functions that aren't needed and can be exploited by an intruder into working to defeat the device's security measures. Once a thief captures and decrypts one PIN block, it becomes trivial to decrypt others on a network.

Other kinds of attacks occur against PINs after they arrive at the card-issuing bank. Once encrypted PINs arrive at the HSM at the issuing bank, the HSM communicates with the bank's mainframe system to decrypt the PIN and the customer's 16-digit account number for a brief period to authorize the transaction.

During that period, the data is briefly held in the system's memory in unencrypted form.

Sartin says some attackers have created malware that scrapes the memory to capture the data.

"Memory scrapers are in as much as a third of all cases we're seeing, or utilities that scrape data from unallocated space," Sartin says. "This is a huge vulnerability."

He says the stolen data is often stored in a file right on the hacked system.

"These victims don't see it," Sartin says. "They rely almost purely on anti-virus to detect things that show up on systems that aren't supposed to be there. But they're not looking for a 30-gig file growing on a system."

Information about how to conduct attacks on encrypted PINs isn't new and has been surfacing in academic research for several years. In the first paper, in 2003, a researcher at Cambridge University published information about attacks that, with the help of an insider, would yield PINs from an issuer bank's system.

The paper, however, was little noticed outside academic circles and the HSM industry. But in 2006, two Israeli computer security researchers outlined an additional attack scenario (.pdf) that got widespread publicity. The attack was much more sophisticated and also required the assistance of an insider who possessed credentials to access the HSM and the API and who also had knowledge of the HSM configuration and how it interacted with the network. As a result, industry experts dismissed it as a minimal threat. But Steel and others say they began to see interest for the attack research from the Russian carding community.

"I got strange Russian e-mails saying, Can you tell me how to crack PINs?" Steel recalls.

But until now no one had seen the attacks actually being used in the wild.

Steel wrote a paper in 2006 that addressed attacks against HSMs (.pdf) as well as a solution to mitigate some of the risks. The paper was submitted to nCipher, a British company that manufactures HSMs and is now owned by Thales. He says the solution involved guidelines for configuring an HSM in a more secure manner and says nCipher passed the guidelines to customers.

Steel says his solution wouldn't address all of the types of attacks. To fix the problem would take a redesign.

But he notes that "a complete rethink of the system would just cost more than the banks were willing to make at this time."

Thales is the largest maker of HSMs for the payment-card and other industries, with "multiple tens of thousands" of HSMs deployed in payment-processing networks around the world, according to the company. A spokesman said the company is not aware of any of the attacks on HSMs that Sartin described, and noted that Thales and most other HSM vendors have implemented controls in their devices to prevent

such attacks. The problem, however, is how the systems are configured and managed.

"It's a very difficult challenge to protect against the lazy administrator," says Brian Phelps, director of program services for Thales. "Out of the box, the HSMs come configured in a very secure fashion if customers just deploy them as is. But for many operational reasons, customers choose to alter those default security configurations — supporting legacy applications may be one example — which creates vulnerabilities."

Redesigning the global payment system to eliminate legacy vulnerabilities "would require a mammoth overhaul of virtually every point-of-sale system in the world," he says.

Responding to questions about the vulnerabilities in HSMs, the PCI Security Standards Council said that beginning next week the council would begin testing HSMs as well as unattended payment terminals. Bob Russo, general manager of the global standards body, said in a statement that although there are general market standards that cover HSMs, the council's testing of the devices would "focus specifically on security properties that are critical to the payment system." The testing program conducted in council-approved laboratories would cover "both physical and logical security properties."

Photo: redspotted/Flickr

See also:

- Part I: I Was a Cyber Crook for the FBI
- Part II: Tightening the Net on Cybercrime
- Part III: The Boards Come Crashing Down
- Sidebar: Tracking the Russian Scammers

Redesigning the global payment system to eliminate legacy vulnerabilities "would require a mammoth overhaul..."