Anatomy of Modern Bank Robberies: Proof Why PIN Protection and KeyBlocks are Important

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

In this article, we explain how compromising the PIN of a customer's prepaid debit card may lead to catastrophic losses for a bank and why it is so important to protect their data. We will analyze two ATM "cash-out" hacking stories that are linked to prepaid debit cards and explain why these frauds could have been prevented if Atalla technologies had been used.

HSMs aren't just needed "because of PCI-DSS requirements," which do not explicitly require the use of HSMs. Today, for Fintech companies (and everywhere else as well) penetration or intrusion testing is part of the enterprise culture. Cryptography, encryption, norms, using FIPS-140 security-evaluated products are just "routine."

Unfortunately, when it comes to real situations, that "routine" is not enough. The IT of banks and more generally, Fintech companies, are protected for a good reason. There are "real" fraudsters and bank robbers out there. The difference is that these robbers won't operate with masks and guns but rather with a keyboard, a mouse, a screen, and internet access. Similar to how trucks carrying cash to and from the banks are armored and protected by guards wearing bulletproof jackets and guns, financial networks are protected by cryptographic systems, passwords, and PINs.

Anyone involved in IT security in banks or processing companies should always keep in mind that the system he or she works for hasn't been designed and created by accident. It has been built to address attacks and robberies, and some of these attacks may be quite sophisticated.

In the two examples we will analyze, the robbers targeted what can be considered as the "Achilles heel" of the banking industry: *prepaid debit cards*. These cards are not linked to any account and have their own balance. They are anonymous and subject to far less monitoring than the other credit or debit cards.

1 The RBS Cash-Out Attack of 2008

The RBS cash-out attack of 2008 was performed by a group of men from Estonia, Russia, and Moldova who hacked into Royal Bank of Scotland's credit card processor, Worldpay. The gangsters started by remotely entering into the computer system of Worldpay.

One of the hackers discovered a vulnerability in the network of RBS Worldpay and started to form an association with other criminals, especially one who had knowledge of cryptography. Using remote access, the hackers were able to break the encryption used by Worldpay because apparently some of their HSMs were poorly configured. It's obviously not an easy hack to perform, but such attacks do exist.

The tracks of the cards were deciphered. However, even worse, the PINs of the cards were also discovered. It is alleged that techniques like trying 2 PINs per card over the database were used in combination with a botnet. After all, PINs are usually 4 digits with 9999 possible values. Therefore, we can compute the probability p=p(N) of getting one right PIN with 1 or 2 tries per card[1] for N cards tested, using the assumption that PINS are uniformly distributed so that a batch of 9999 cards have all different PINs:

- p$\sim$N/9999 for 1 try per card
- p$\sim$2N/9999 for 2 tries per card

The computation with one try is easy : we have probability 1/9999 to find a matching PIN with first card and probability 9998/9999 not to find the matching PIN... in such a case we have probability 1/9998 to find a matching PIN with second card and probability 9997/9998 not to find, and so on. By taking the sum over all the branches of the possibility tree we get :

p=1/9999+(9998/9999)$*$(1/9998)+(9998/9999)$*$(9997/9998)$*$(1/9997)+... = N/9999

The computation with two tries is slightly more complicated.

We have probability 1/9999+1/9998 to find a matching PIN in the first card and probability (1-1/9999-1/9998) *not* to find a matching PIN , then in such case we have probability 1/9997+1/9996 to find a matching PIN in the second card and probability (1-1/9997-1/9996) *not* to find a matching PIN etc... at the kˆth branch of the possibility tree, we are at the kˆth card with probability 1/(9999-2k)+1/(9999-2k-1) to find a matching PIN and probability 1-1/(9999-2k)-1/(9999-2k-1) *not* to find a matching PIN.

The required probability p(N) is the sum of all the partial probabilities, that is to say

[1] 2 being the maximal possible number of tries before the card would be blocked and raise attention

p=1/9999+1/9998
+ (1-1/9999-1/9998) ∗(1/9997+1/9996)
+(1-1/9999-1/9998)∗(1-1/9997-1/9996)∗(1/9995+1/9994)
+....
+(1-1/9999-1/9998)∗(1-1/9997-1/9996)∗...∗(1-1/(9999-2N)-1/(9999-2N-1))∗(1/(9999-2N-2)+1/(9999-2N-3))

This means that approximately for every 5,000 cards tested, one PIN will be found.
The hackers found 44 PINS linked to 44 accounts. This implies that they allegedly tested approximately 200,000 cards. Using the HSM that they could access, they managed to raise the withdrawal limits of the corresponding accounts, and then increase the balance of the cards.

Once they had the PINs, they created cloned cards using magnetic stripe encoders (non-EMV cards). They then hired “mules" that cashed the cards in several countries. Their crews withdrew $9 million in more than 2,100 cash machine transactions worldwide in less than 12 hours.The loss and harm significantly damaged the reputation of the Royal Bank of Scotland.

2 The RAKBank and the Bank Muscat Cash-Out Attack of 2012 and 2013

The circumstances behind the robberies committed against the Bank Muscat of Oman and the RAKbank (National Bank of Ras Al-Khaimah in the United Arab Emirates) are very similar.

A Turkish hacker named Findikoglu gained access to the networks of certain prepaid debit card payment processors, namely, ElectraCard from 2010 to 2013. The access was used to fraudulently obtain accounts and PINs. Card limits were suppressed while a network of “cashiers" operated all over the world to “cash-out" money at ATMs.

Following these attacks, the Bank Muscat of Oman suffered a loss estimated at $40 million spread over 36,000 fraudulent ATM transactions. The RAKBank suffered $9 million in losses.

Security experts commented that if criminals manage to break into servers at a bank, and gather account data and, especially, PIN numbers, there isn’t anything as far as they knew that could be on a device on the other end to stop the attack from happening.

3 How to Protect Debit Cards

In the aforementioned attacks, the cybercriminals operated like a well-oiled mechanism:

1. They found a security breach in a payment processor network;
2. They infiltrated financial institution(s) to find matching PINs and accounts data;
3. They changed the balances and removed the transaction limits of compromised cards;
4. They cloned the cards ('carders');
5. They hired cashiers ('mules') to cash-out at ATMs using the cloned cards;
6. Eventually, they erased the logs to cover their tracks

Here we are talking about non-EMV cards that are still widely used in many countries. However, there are several ways that an EMV chip can be destroyed to force the use of an EMV card's magnetic stripe ('EMV fallback').

Without knowing PINs, none of these crimes could have been accomplished. Therefore, it is fundamental to prevent access to the HSM to protect PINs and prevent unsecured PIN verification.

As exhibited above, any access to a network, even partial, could allow attackers to "guess" the PINs of some cards through a comparison technique and by using PIN verification over a database of cards.

PIN verification API should only be reachable from secure systems like Atalla HSMs do.

These HSMs can only be accessed remotely via the Atalla Secure Configuration Assistant that uses newer, and very secure smartcards for authentication. Using the AKB (Atalla Key Block) could prevent many of these attacks from happening.