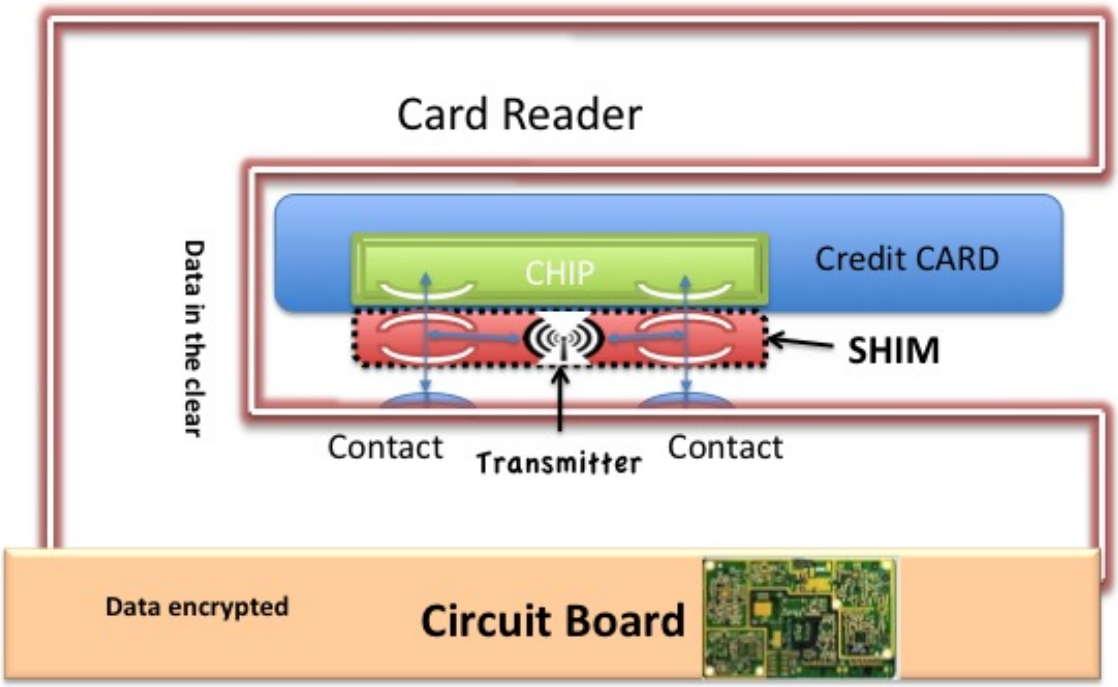
>
Published on *NetworkWorld.com Community* (http://www.networkworld.com/community)

Newest Attack on your Credit Card: ATM Shims

By *jheary*
Created *Jul 11 2010 - 3:31pm*

Shimming is the newest con designed to skim your credit card number, PIN and other info when you swipe your card through a reader like an ATM machine. The shim is the latest attack being used by criminals to steal your credit card info at the ATM or other Pin Entry Device. According to Diebold, " The criminal act of card skimming results in the loss of billions of dollars annually for financial institutions and card holders. Card skimming threatens consumer confidence not only in the ATM channel, but in the financial institutions that own compromised ATMs as well."

Shimming works by compromising a perfectly legitimate card reader (like an ATM) by inserting a very thin flexible circuit board through the card slot that will stick to the internal contacts that read card data. The shim is inserted using a "carrier card" that holds the shim, inserts it into the card slot and locks it into place on the internal reader contacts. The carrier card is then removed. Once inserted, the shim is not visible from the outside of the machine. The shim then performs a man-in-the-middle attack between an inserted credit card and the circuit board of the ATM machine. See the image below for an example of what a skim looks like inside the ATM.



Before it was practical/possible to create shims, thieves used various skimmer designs that attached to the outside of the card slot. Like the one shown below:
Image is Courtesy of Naples Police Department:

It is important to keep in mind that this attack is not trivial from an engineering standpoint. The shim needs to be extremely thin and flexible. In fact it must be less than 0.1mm in most cases to fit in the space allocated in the card reader and not obstruct credit cards from being inserted seamlessly. The EMV 4.2 standard [1] that regulates the dimensions of the card slot calls for the following specifications according to section 5.2.1.1 on Module Height:

> *The highest point on the IC module surface shall not be greater than 0.10mm above the plane of the card surface.
> *The lowest point on the IC module surface shall not be greater than 0.10mm below the plane of the card surface.

To put in perspective how thin less than 0.1mm is, think about this. Your credit card is 0.76mm thick. A grain of salt is 0.5mm thick. The human hair is about 0.18mm thick. The smallest objects that the unaided human eye can see are about 0.1 mm long. Now that's thin!!!! Add to this that the shim must be semi-flexible and this attack becomes quite a technological achievement.

Recent advances in microchip fabrication coupled with the commoditization of same means that shims this size can be cheaply and reliably manufactured by the bad guys. The actual designing of the shim and its components, especially the transmitter function, is still non-trivial. But it was inevitable that this the thieves would figure this out, as they have. It has been found that effective flexible shims are recently being mass produced and widely used in certain parts of Europe.

One of the main reasons this attack can succeed is because in most all countries today (like the U.S.A) the data sent from the chip on a credit card to the contacts on the ATM circuit board is sent in the clear. So if you can get in the middle of that data flow, like a shim attack does, you can capture card data, pin information, CVV info, etc. However, most Pin Entry devices have supported offline-encrypted pin (encrypting the data between chip and board) for years. So it is possible that if this feature was enabled on both the credit card and the machine it could defeat this attack. The credit card chip encrypts the data using its public key before it sends it to the card reader.

Skimming is not something new, it's been around since ATM machines. However, it is continuing to

become more sophisticated and readily available. It is a constant battle between the Pin entry device manufacturers and the criminals. The shim attack is just the latest in a long history of attacks. For a look at some other attacks from the past and present see my other article on this topic here. [2]
Diebold released five new anit-skimming protection levels for its ATM devices june 1st 2010. You can read about it here: http://www.news.diebold.com/article_display.cfm?article_id=5065 [3] Unfortunately, none of these helps with the shim skimming attack. That problem has yet to be solved mechanically yet.

For information on how to protect yourself from skimming attacks see here http://masteryourcard.com/blog/2009/08/24/how-to-protect-yourself-from-c... [4]

Great article from Cambridge University researchers on security flaws in Pin Entry Devices: http://www.scribd.com/doc/6444475/UCAMCLTR711 [5]

The opinions and information presented here are my PERSONAL views and not those of my employer. I am in no way an official spokesperson for my employer.

More from Jamey Heary:

* Credit Card Skimming: How thieves can steal your card info without you knowing it [2]
* Google Nexus One vs. Top 10 Phone Security Requirements [6]
* Why you should always shred your boarding pass [7]
* Video rental records are afforded more privacy protections than your online data [8]
* The truth about new SSL attacks [9]
* 2009 Top Urban Legends in IT Security/a> [10]

Go to Jamey's Blog [11] for more articles on security.

Shim attack doesn't actually compromise chip cards

By Anon (not verified) on Mon, 07/12/2010 - 9:25am.

Chip cards generate a different cryptogram for every transaction, using internal keys and unique transaction data produced by the terminal. So skimmed data can't be used to create fraudulent chip cards (as the chip keys can't be skimmed) or even replay chip transactions.

Note: The 0.1mm EMV requirement is the maximum thickness of the card's chip, NOT the maximum reader slot size. EMV doesn't define the maximum allowable thickness of the card reader slot, so the shim can likely be thicker than 0.1mm - it really depends on the vendor's card reader design.

not implemented widely

By jheary on Mon, 07/12/2010 - 2:31pm.

As I pointed out in the article, You are correct in that it is possible to encrypt from the chip to the reader. This is a good defense against the basic shim attack I went through. However, as I pointed out in the article, encryption between the chip and reader is very rarely deployed. So today the shim attack is very much a real attack. Also, even when deployed with encryption the reader will allow fall back to non-encrypt and

even magstrip. So the shim, being man-in-the-middle would simply intercept the 0x03 code from the chip that tells the reader to expect encryption and then change it to 0x01 forcing the use of unencrypted transfer.

-Jamey

Chip data is never encrypted, only the PIN

By Anon (not verified) on Mon, 07/12/2010 - 11:45pm.

Data exchanged between the chip and reader is never encrypted. Only the PIN can be encrypted, if supported by both the card and reader. You're absolutely right that the shim could fool the reader into using plaintext PIN (even if the card supports encrypted PIN).

However, my point is that captured chip data is useless to the attacker, since the cryptogram can only be used once. In addition (unlike magstripe cards) captured chip data can't be used to create a fraudulent chip card, since the keys are protected within the chip. You couldn't create a fraudulent magstripe card either, since the full magstripe data is never stored in the chip.

RFID

By Anon (not verified) on Mon, 07/12/2010 - 2:17pm.

So, the next evolution in ATM cards should be Encrypted near-field RFID.

What kind of card?

By Anon (not verified) on Mon, 07/12/2010 - 2:20pm.

So, what kind of ATM card is this? There are no contacts on my ATM card...it uses a magnetic strip. Looking at the picture above, it looks like this attack is targeting those credit/ATM cards that have a smart chip on them. I don't see how this thing will work with a magnetic strip card.

Isn't credit a man-in-the-middle-attack?

By Anon (not verified) on Mon, 07/12/2010 - 3:10pm.

Given the global history of power and wealth, why haven't we learned that any system that ties daily needs with an arbitrary object are magnets for criminals? It's not as if human behavior is a big secret...

The contactless smartcard

By olesmartie (not verified) on Mon, 07/12/2010 - 8:26pm.

The contactless smartcard transit industry has been using reasonable secure mutual authentication schemes since the early 90s (not including the mifare Classic here). When is the banking industry going to catch up?

Cisco Security atm security atm shim credit card attack credit card security credit card shim credit card shimming credit card skimming Heary Jamey Heary security shimming

---

Source URL: http://www.networkworld.com/community/blog/newest-attack-your-credit-card-atm-shims

Links:

[1] http://www.emvco.com/specifications.aspx?id=155
[2] http://www.networkworld.com/community/node/33210
[3] http://www.news.diebold.com/article_display.cfm?article_id=5065
[4] http://masteryourcard.com/blog/2009/08/24/how-to-protect-yourself-from-credit-card-skimming/
[5] http://www.scribd.com/doc/6444475/UCAMCLTR711
[6] http://www.networkworld.com/community/node/49560
[7] http://www.networkworld.com/community/node/44457
[8] http://www.networkworld.com/community/node/44055
[9] http://
[10] http://www.networkworld.com/community/node/42489
[11] http://www.networkworld.com/community/heary