Hal Berghel

Credit Card Forensics

Decoding the magnetic attraction of criminals to swiping.

A few years ago, local law enforcement brought an interesting question to one of my research laboratories: Why were street criminals carrying around pockets full of hotel room keys? Arrests of the local criminals were producing a virtual cornucopia of hotel room keys of all shapes and sizes. In addition, the police found gift cards, rewards cards, player's cards, calling cards, membership cards—virtually everything that had a magnetic stripe on it.

It turned out that the magnetic stripes contained credit card information. The source data was either "skimmed" or "duped" from the original card and then recorded on the magnetic stripe of hotel room keys with widely available card reader/writers. There was a burgeoning industry in this form of credit card fraud, with well-organized groups working within a moderately well-defined chain of command. The street criminals were collecting the information and passing it up to the criminal leadership who then either imprinted the account information on the room keys, brokered the account information over the Internet, or traded the information with other criminals.

The most prevalent threat was skimming since it doesn't require separating the card from the owner. This produces a much longer useful life for the credit card information—by the time the user or credit card company discovers that the card has been compromised, the thieves have already moved on to the next victim. A common skimming tactic is to "double swipe"—once at the point-of-sale terminal, and once on a handheld device. Current battery-powered skimmers are about the size of a thumb, cost less than $500, can hold thousands of credit cards, and have USB interfaces for ease of downloading. At the time of this investigation, local law enforcement discovered that most of the skimming was taking place in ethnic restaurants. Members of the restaurant wait staff could easily conceal the skimmer in their aprons or pockets and complete a shift with dozens to hundreds of credit cards skimmed.

The first batch of discovered hotel room keys produced some confusion. Local law enforcement was not familiar with seeing so many hotel room keys in the hands of one person. But after the credit card information was discovered, the proverbial light went on. In the state of Nevada it was illegal to possess more than two credit/debit cards in another's

HAL MAYFORTH

name. The criminals knew if they were found with actual credit cards, they would be arrested. So their workaround was to copy the magnetic information onto the surrogate cards to avoid detection and detention. The scheme ended when law enforcement representatives discovered what kind of information was on the hotel room key magnetic stripes.

Digital Crime Scene Investigation

When Deputy Chief Dennis Cobb brought this caper to our attention, he challenged us to develop a handheld scanner that could detect whether anomalous data was on a magnetic stripe without actually reading or storing the data. Legally, knowing *that* there is credit card information on a hotel room key is a very different piece of evidence than knowing *what* credit card information was on it. Our first challenge was to define what it was to be an anomaly in this context.

When IBM created the magnetic stripe card technology in the 1960s it allowed different industries to influence the format of the three tracks on the stripes. The airlines industry got first pick on track one, while the banking community defined track 2 and the savings/thrifts defined track 3. A de facto standard recording density for most industries and applications is 210 bits/inch for all 3 tracks. Track 1 is a 7-bit format, while tracks 2 and 3 are 5-bit. Since track 1 has the larger character set, only it has alphanumeric-cum-special character capability.

Field	Length	Definition	Example
1	1	start sentinel	%
2	1	format code (alphabetic)	B=format code for bank/financial industry
3	<=19	primary account number	121741512345678
4	1	field separator	*
5	<=26	holder's name	sutton/willie
6	4	expiration date (MMYY)	0503
7	3	service code	101
8	5	PIN Verification Value	51395
9	var.	discretionary data	000000000248000000
10	1	end sentinel	
11	1	Longitudinal Redundancy Check Character	1

Example data specifications.

Tracks 2 and 3 are limited to the ASCII hex 30-3f characters. Of course, these formats could vary widely by application.

For brevity, I will focus on the financial industry, and more specifically, on credit cards. There are several ISO/IEC standards that apply to magnetic stripes on credit cards, especially ISO/IEC 7810-7813. The related specification, ISO/IEC 4909, applies to the thrift industry and a similar discussion that is beyond the scope of this column. These standards specify the physical characteristics, layout, track densities and formats, merchant ID codes, and similar elements for financial transactions cards. Of specific interest was ISO/IEC 7813 relating to the data structure and content of magnetic tracks 1 and 2.

Figure 1. View from handheld scanner: looking for hotel room key information but finding credit card information.

Of course there is considerable variety in the data specifications between credit card issuers that must be accommodated when scanning the card; a generic example is shown in the table here. Myriad subtle differences may be found within this generic scheme. Again, for brevity I will only mention that they, too, may be used to authenticate the information as belonging to a credit card. The overarching idea behind this analysis is that the more information on the magnetic stripe that conforms to credit card

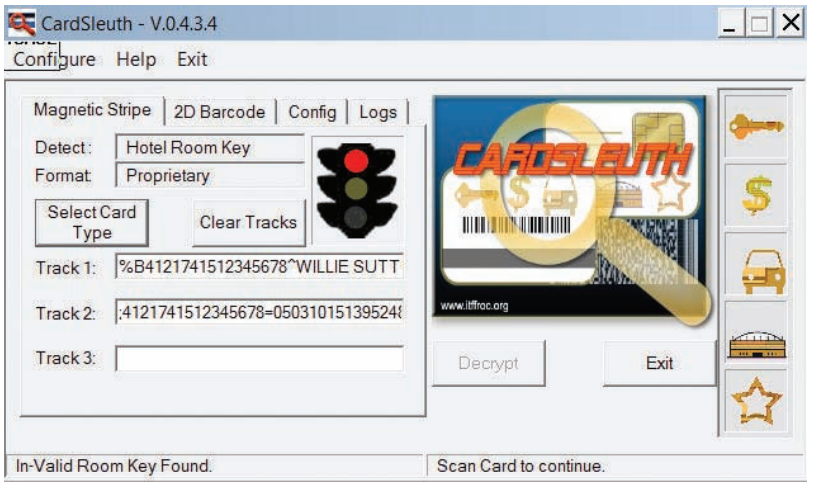
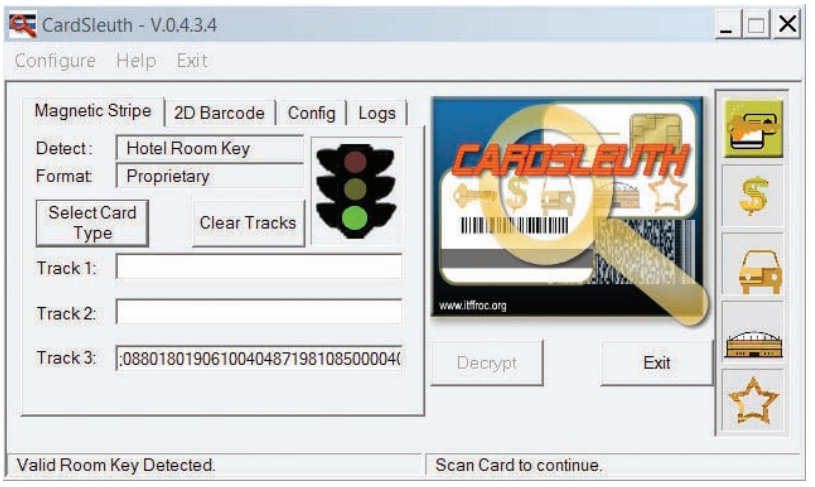


Figure 2. Forensics view of looking for hotel room key information but finding credit card information.

formats, the higher the probability this information is a credit card record. The goal is to provide law enforcement with immediate feedback that produces probable cause for further forensic investigation.

The figures shown here illustrate some of the features of our scanning system, CardSleuth. Note that in Figure 1 only the red stop light is indicated (accompanied by sound in our system), meaning the magnetic stripe scanned is not what would have been expected. In this case, we were looking for hotel room key information on the magnetic stripe, but the red light indicates we found a credit/debit card information. This satisfies our requirement of reporting "that" rather than reporting "what." Figure 2 is the forensics view of the magnetic stripe information—normally seen by detectives after an arrest, court order, or similar legal procedure has been issued. This confirms the format of the data described previously. Figure 3 reports the result of looking for a hotel room key and finding it.

Figure 3. Forensics view of looking for and finding a legitimate hotel room key.



The notion of anomaly deserves further explanation here. Recall that our original goal was to detect anomalies, one example of which is credit card information on a hotel room key. Of course, the converse would also be an anomaly. Though we haven't detected this as yet, it's entirely possible that criminals could put hotel room information on a credit card in order to conceal the fact that they have access to a victim's room. Again, the criminal reasoning would be similar to the "more-than-two" case: if criminal activity were suspected in a hotel room, a holder of a hotel room key to that room might be suspect. But what is the likelihood that an investigator will swipe a worn credit card in a hotel room key?

CardSleuth is designed to look for such anomalies on a variety of cards with magnetic stripes, barcodes, and RFID elements. The Cartesian product of these media types against function or use (for example, credit/debit/ATM cards, driver's licenses, sundry identification cards, passports, visas, room keys, benefit transfer cards, and so forth) significantly complicate the notion of "anomalous." In this column, I discuss just one case.

The Rest of the Story

URL PEARLS

For more information about credit card theft issues discussed in this column, see Brian Krebs's *Washington Post* blog at http://blog.washingtonpost.com/securityfix/2006/03/street_level_credit_card_fraud.html.

For curious readers, ISO/IEC 7810 documentation may be found on the ISO/IEC/IEC Web site at www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail? CSNUMBER=31432&ICS1=35&ICS2=240&ICS3=15. For those who prefer not to pay for the download, a useful facsimile is available online at the DED Limited Web site at www.ded.co.uk/magnetic-stripe-card-details.html; http://www.asciitable.com/ is a convenient online ASCII table.

Our anti-spoofing technology extended to counterfeit and forged IDs as well. The problem of fungible credentials is discussed in my December 2006 column.

Periodic review of popular government and law enforcement Web sites that deal with preventive measures for electronic crime and identity theft is definitely warranted, as current loss estimates exceed $100 billion and affect a large percentage of the population. A good start is the Department of Justice Web site, particularly www.usdoj.gov/criminal/fraud/websites/idtheft.html. Another useful reference is the Internet Crime Complaint Center at www.ic3.gov. A first approximation at securing credit card transaction processes can be found in the Payment Card Industry (PCI) Data Security Standard; version 1.1 (Sept. 2006) is available at

There is considerable general awareness of the hotel room key card scam in my Las Vegas municipality, but it's not dead yet. Not all municipalities and their law enforcement have the same levels of awareness of this exploit. Further, variations abound. The most interesting aspect of this story was how a law enforcement agency and a university research center could cooperate to prevent crime.

In the course of this project we came up with some interesting observations. For one, the entire scam could have been avoided if the scanners were configurable with respect to the acceptable level of coercivity on the magnetic stripes. Financial industries use the more persistent and more reliable high-coercivity magnetic stripes with a flux density of 4,000 Oersteds. All of the hotel room keys that were provided to us were low-coercivity (300 Oersteds). The difference in magnetic field strength is easily recognizable by modern electronics. In our case, simply rejecting any credit card information that appeared on a low-coercivity magnetic stripe would have prevented the problem from arising in the first place. Note that a "low-coercivity" block on unattended point-of-sale terminals could have prevented this criminal behavior before it got started.

Another by-product of our work was the prevalence of credit card information on the Internet. At one point we were experimenting with Net bots that could look for and report on financial card information on the Net. As an aside, I can affirm that this research was of little interest to law enforcement for legal reasons. Ironically, having the ability to find credit card fraud in progress incurs considerable liability to attempt to thwart it, which introduces issues of agency, jurisdiction, work flow, and so forth, and invites new problems struggling law enforcement agencies with enormous case loads are ill-prepared to handle.

Over time, this project has been extended to other identification and card media formats, and functionality that goes beyond law enforcement. The common theme, however, is the detection of anomalous information on widely used identification and access control media.

CONCLUSION

I would be remiss if I didn't suggest some guidelines to protect oneself from scams such as those described in this column. The U.S. Department of Justice's SCAM acronym is appropriate here: be Stingy about giving out personal information, Check personal financial information regularly, Ask for copies of personal credit reports periodically, and Maintain careful records of banking and financial accounts. C

HAL BERGHEL is associate dean of the Howard R. Hughes College of Engineering at the University of Nevada-Las Vegas, the director of the Center for Cybersecurity Research (ccr.i2.nscee.edu), and co-director of the Identity Theft and Financial Fraud Research and Operations Center (www.itffroc.org).

© 2007 ACM 0001-0782/07/1200 $5.00