Digital Village

Hal Berghel

Fungible Credentials and Next-Generation Fraud

Digital technology is easing access and lowering barriers for a new generation of criminal.

One of the most dramatic effects of global digitization is the transformation of white collar crime. Computer and network technology makes it possible for the white collar criminal to operate more efficiently with less risk and near total geographical independence. It has long been suspected that the economic impact of white collar crime surpasses its blue collar counterpart. The consensus seems to be that white collar crime venues such as embezzlement, theft of negotiable instruments, misappropriation of funds, insider trading, income tax fraud, theft of trade secrets, violation of intellectual property laws (patents, copyrights, trademarks, and so forth) have produced more economic damage by far than more mundane counterparts like burglary, auto theft, forgery, robbery, and vice for a very long time (think Enron and Worldcom). The difficulty in quantifying the losses due to these crimes is primarily due to low frequency of reporting.

The digital twist is the increased accessibility of electronic white collar crime. The criminals seem to have the same socioeconomic advantage as white collar criminals of yesteryear, but the entry-level barriers are much lower. The Nigerian Scam (aka, "advance fee fraud," "419 fraud") is indicative of the ease with which neophyte computer users may cause billions of dollars of worldwide economic damage with only a primitive telecommunications and networking infrastructure at their disposal.

One of the most troublesome applications of computing technology to white collar crime for law enforcement is fungible credentials.

Fungibility

The operative meaning of 'fungible' in this context is "interchangeable." As I use the term here, fungible documents include counterfeits (for example, currency), forgeries (contracts, negotiable instruments, signatures), as well as a third category that I call "quasi-verifiable" or "legitimized." Most fungible documents are created for criminal purposes, usually with the intent to defraud. "Legitimized" documents are those produced by legitimate issuing authorities based upon false information. One example is a driver's license that has been issued to an individual under a fictitious name. That's where the quasi-verifiable characteristic comes in. The driver's license cor-

PEP MONTSERRAT

responds to a Department of Motor Vehicles (DMV) database record—in that sense it's legitimate. However, the data fields do not correspond to the holder—both the credential and the credentialed are real, they just don't correspond to each other.

The driver's license is an important member of the set of core credentials in the U.S. (along with birth certificate, passport, and Social Security number). It is particularly valuable because it is the most widely circulated of the credentials that have an image or likeness of the holder. In all 50 states, if you're going to operate a motor vehicle on a public road, you must have one. For this reason, it is a tempting target for counterfeiters. Figure 1 shows two counterfeit driver's licenses manufactured for the same person to establish dual identities (both of which were fictitious, incidentally).

Counterfeiting driver's licenses has become a cottage industry in the U.S. Law enforcement sees the entire spectrum from simple laminates of dot matrix printings to sophisticated replicas—typically those that have the authentic 45-degree hologram laminates superimposed on legitimate, stolen card stock printed with the same equipment that DMV uses. Figure 1 falls somewhere on the lower end of the quality spectrum: better than one produced in a college dorm room, but unable to withstand the scrutiny of law enforcement.

There are several features of these counterfeits that betray poor quality. For one, the 45-degree laser hologram laminate is missing. This is the easiest to spot even with minimal illumination. Second, the state seals along the bottom are blurred and suggestive of a low-resolution background image. Third, the two microprinted visible watermarks that appear on authentic Nevada driver's licenses of the period are missing.

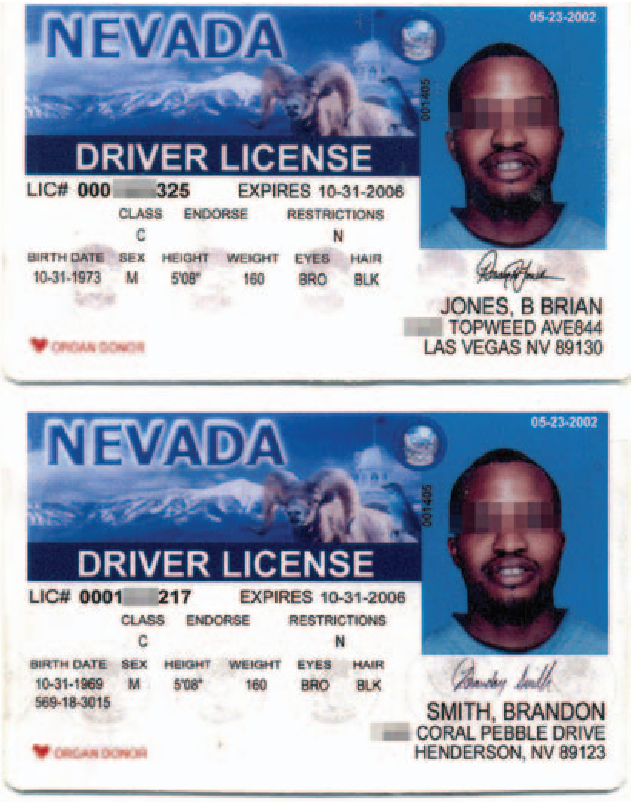

Figure 1. Two counterfeit driver's licenses for the same person. (Both identities are fictitious; pixilation added by author.) Source: Las Vegas Metropolitan Police Department.

The Science of Securing Credentials

The act of counterfeiting core credentials is so widespread at this point that an entire industry has arisen to reduce exposure. The taxonomy of anti-counterfeiting technology shown in Figure 2 is derived from Michael Gips's white paper, "The Spurious and the Injurious" (see www.security-management.com/library/001540.html).The features that apply to the analysis of the counterfeit driver's licenses in Figure 1 appear in boldface type in Figure 2. The taxonomy illustrates the considerable lengths that various government agencies and manufacturers have gone to discourage counterfeiting. Rigorous authentication technology also motivates criminals to seek means to obtain legitimized credentials.

There is also a fourth deficiency that is more subtle and doesn't apply to the taxonomy: the addresses are both bogus. The reader may be amused to see the satellite photo of the area in which the Topweed Avenue address would fall in Figure 3. Not only is the address number bogus, but there are no apartment building within sight—certainly none with 844 units.

Next-Generation Fungibility and Credential Amplification

The typical criminal would use fungible credentials as an instrument to defraud because it offers reduced risk, minimal effort, and increased effectiveness. Financial frauds, money laundering, and identity theft are three common exploits that typically rely on fungible credentials. Fungible credentials are useful precisely because they simultaneously obscure the criminal's real identity and facilitate any authentication that may be required.

A very common illustration is the use of fungible IDs to authenticate credit or debit card transactions. Merchants routinely rely on the photo and name on driver's licenses to authenticate the card holder. Thieves find fungible IDs to be ideal companions to stolen credit/debit cards in committing fraud. Counterfeit driver's licenses have proven to be quite effective for small to medium-sized purchases.

However, the counterfeiters are becoming the bottom feeders in the credit card fraud food chain. In order to see why, we need to add another level of complexity to our analysis. Counterfeit IDs may be thought of as 'limited use" vehicles of authentication: they have a fundamental defect: its issuance itself cannot be verified, and thus won't withstand any level of official inspection—for example, a simple records check during a routine traffic stop. To overcome this defect, more sophisticated criminals are using legitimized credentials. This is where the upper echelon of "new millennium fraudsters" are headed, and it's causing headaches for law enforcement agents.

1. Overt Methods

- a. Optically variable devices
    - i. Holograms
    - ii. Kinegrams
    - iii. Optical variable (aka color-shifting) inks
    - iv. Visible watermarks
        - **1. official seals**
        - 2. ghosting
        - 3. shadowing
        - **4. microprinting**
- b. Machine-readable media
    - i. Magnetic stripes
    - ii. Bar codes
        - 1. 1-Dimensional
        - 2. 2-Dimensional
    - iii. Smart cards
- c. Numbering
    - i. Serial numbers
    - ii. Unique IDs
        - 1. original
        - 2. derived (for example, SSN)
    - iii. Transaction numbers

3. Covert Methods

- a. Special inks
    - i. Thermochromic
    - ii. UV
    - iii. Infrared
    - iv. Water-fugitive
    - v. Hard-to-reproduce
    - vi. Reactive
- b. Special Printing methods
    - i. intaglio/gravure
    - ii. Microprinting
    - iii. Prismatic
    - iv. Altered fonts
    - v. Security indicia
    - vi. Void pantographs
- c. Limited distribution media
    - i. Special paper
        - 1. safety papers
        - 2. chemically coated paper
        - 3. anti-washing paper
        - 4. chemically reactive/non-reactive paper
    - **ii. embedded laminates (for example, hologram, kinegram)**
- d. RFID tags

3. Forensic Methods

- a. Microtaggants
- b. Molecular markers

Figure 2. Taxonomy of anti-counterfeiting technology (derived from Michael Gips's white paper, "The Spurious and the Injurious"; see www.securitymanagement.com/library/001540.html).

Credential Amplification

The starting point of a legitimized credential remains the counterfeit document. However, the counterfeit is only the means to the end of obtaining a legitimized document. A typical scenario might be to begin by ordering a counterfeit passport from people who linger around the dark side of swap meets. It's not uncommon for criminals to special order the passports by country, name, visas, and endorsements. The counterfeit passport is then used in the "credential amplification" phase to produce the tokens that will be actually used to defraud, for example, a driver's license issued by DMV. The typical DMV has no means to validate passports, so the amplification is relatively straightforward. The driver's license may in turn be used to obtain a Social Security number, county health card, and other documentation until the wallet is filled. It goes without saying that the variations on this theme seem endless.

What is unique to the credential amplification approach to fraud is that the legitimized token becomes 'authenticatable'—that is, there is actually a DMV record for the name on the driver's license. This is usually all it takes to establish a solid false identity (or steal someone else's). As a reality check, contact your local bank and ask what identification is required to open an account, withdraw from an account, establish a credit line, or obtain a credit/debit card. In many if not most cases, only two forms of ID are required, only one of which must have a photo and neither of which are validated beyond visual inspection, a valid driver's license (in precisely the sense that I mean "quasi-verifiable" or "legitimized"), a state-issued or military ID, or a U.S. Passport.

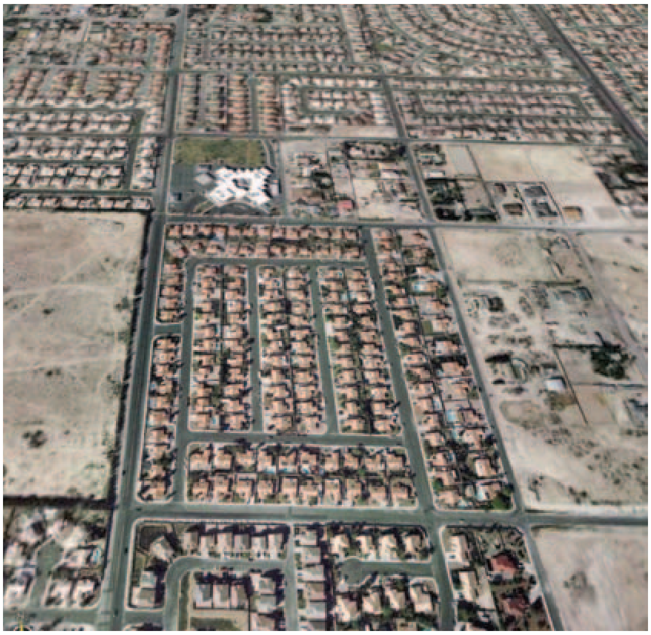

Figure 3. A satellite image of the Topweed neighborhood (mid- to lower center). Note absence of apartment buildings. (Produced with Keyhole 2 PRO. © 2004 Keyhole Corporation.)

Conclusion

In the past few years, the use of fungible credentials has taken a turn for the worse from a social perspective. Since many criminals only use the counterfeit credentials to obtain quasi-verifiable credentials in the amplification phase, the original counterfeits are disposable. The operative token credentials are legitimately issued by agencies. This makes detection nearly impossible, for the token (if not the holder) is legitimate. Note how this circumvents the anti-counterfeiting technologies mentioned previously, unless all government agencies and law enforcement are postured to authenticate all documents, irrespective of source. This isn't likely to happen any time soon.

While the problem of counterfeiting is not new, the ease and quality with which counterfeit credentials may be produced with modern computer and printing technologies is new. Arrests of

URL PEARLS

The Nigerian Scam is the stuff of which a dime store novel is made: corruption, intrigue, murder, mayhem, and that's just the introduction. Observed variations of the Nigerian Scam carry names like the "overinvoiced contract," the "trade default," the "bequest," the "wash-wash," and the "spoof bank," to name but a few. "Bequest" scams, in turn, include "advance fee," "transfer tax," and "performance bond" tactics, and so forth. It is truly remarkable how much has been garnered from this sub-cerebral exercise. Incidentally, the label "419 (four-one-nine) fraud" is derived from the section of the Nigerian penal code that covers this type of fraud. For further information, see the 419 Coalition Web site at home.rica.net/alphae/419coal/, or the U.S. Department of State Web site at www.state.gov/www/regions/africa/naffpub.pdf. The link to the U.S. Secret Service "Operation 4-1-9" report at www.secretservice.gov/alert419.htm appeared to be broken when this column was written, but cached copies remain available (for example, cc.msnscache.com/cache.aspx?q=3910458378891&lang=en-US).

Driver's license security features run the gamut from the pedestrian to the downright stealthy. There are several ways to categorize these features: overt vs. covert, optical vs. machine readable, forensic vs. non-forensic, so a precise taxonomy is beyond the scope of this column. Interested readers should consult the American Association of Motor Vehicle Administrators Web site at www.aamva.org/ (search for "id design"). The standard reference for current practices is the I.D. Checking Guide (idcheckingguide.com), although private copies may be difficult to obtain.

identity thieves and credit/debit card fraud rings almost always yield a computer and a good-quality dot matrix printer. Today, one can enter the ranks of the successful fraud criminal for a few hundred dollars. With judicious use of credential amplification and some street smarts, one can quickly leverage this minimal investment into a move into the defrauding big leagues.

The point to bear in mind is that this new cottage industry within our global digital village has been made possible by high-quality, inexpensive computers, printers, and small office/home office software. Ironically, the production of large quantities of fungible credentials is a direct consequence of the same computing appliances and productivity applications that have made modern business so efficient. Perhaps the scariest application of fungible credentials to date is the counterfeiting of law enforcement IDs by posers for home/office invasion.

Look for the problem of fungible IDs to obey Moore's Law in the years to come. 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 Cybermedia Research (ccr.i2.nscee.edu), and co-director of the Identity Theft and Financial Fraud Research and Operations Center (www.it.ffroc.org).

This column is a byproduct of research conducted at the Identity Theft and Financial Fraud Research Center in conjunction with the Las Vegas Metropolitan Police Department. I appreciate the assistance of Michael Sthultz and my LVMPD colleagues Deputy Chief Dennis Cobb, and Detectives Kai Degner and D.C. Tony in developing material for this column.