JIBC Editorial: No Barriers to Security

By Martin Nemzow
Network Performance Institute
Miami, FL 33141
www.networkperf.com
mnemzow@networkperf.com

Mr. Nemzow has consulted in high-tech for 20 years, assisting several achieve IPO status. He has been active in marketing, commercial banking, insurance, and software development on personnel, strategy, financial, technology implementation, manufacturing, and day-to-day operational matters. As president of Network Performance, which is deploying a new paradigm for international currency translation and time-independent accounting, he holds several patents on those processes. He is the author of 20 McGraw-Hill books, including the bestselling McGraw-Hill books Web Video Complete and Ethernet Management Guide, 3rd Ed. online and top-selling ecommerce book, Building Cyberstores or construccion dé Ciberalmacenes. You also can read his ecommerce-business columns for WebServer Magazine online at http://webserver.cpg.com. For more information see http://www.networkperf.com/marty.htm.

A serious project assessing biometric input and authentication devices recently diverted me away from normal tasks. This story is not about biometrics, but rather about the abject failure of barrier-based security. I say his because I am well-versed in server farms and firewalls and the penetrations that make customers skittish, banks terrified, and unnerve management and operations staff with extended downtimes of their critical 7x24 services. This should have special interest to all JIBC readers planning or implementing online ventures. Specifically, this story is a contrast of the machinations used to create firewalls, user protections, Internet and Intranet defenses against the accidental efforts of open source programmers, the intensive activity of hackers, and by those with even more perverse intentions to thwart security. The technical details are important in the story and develop the logic behind my meager assessment of current security and prospects in the future.

Various biometric devices that I bought and paid for created device drivers conflicts; they did not conform with the industry-standard BAPI (Biometric Application Programming Interface) despite assertions from marketing people and technical support. As luck rescued me, Fortune Magazine and Tandy Radio Shack are running a campaign for the :CueCat barcode reader. At this time too, American Express has introduced Blue (a credit card) along with a free magnetic stripe and Smart Card Reader when your signup for it online. I applied for a AMEX Blue card and got :CueCat readers from both Fortune and at Radio Shack during visits to buy several cellular phones. After 23 days of playing games with AMEX card services technical support I had a card reader (not USB as ordered but a serial port unit) but still no access to my account online. I know the 1-800 AXP-1234 support number from calling from the office on from the road so many times. The system and various helpful people kept resetting my password (unbeknownst to me) thus locking me out of the online site; apparently, I also kept choosing passwords longer than 10 letters and digits. The web site would accept and confirm my passwords but later fail actual login because the site password limitation was set at 8 letters and numbers even though this was undocumented. What was worse, some site function logins would accept me, others not; site-wide, services were inconsistent.

This is a prime example of a major service provider not debugging or checking workflow sufficiently, and then failing over a period of 23 days to recognize and solve the programming script errors. The customer support debacle is a different story with ramifications for profits and success in online banking and financial services; it is appropriate to ecommerce planners, but not to the focus of this article. With the hardware in my hands, I was blue in the face while resolving conflicts with USB ports, parallel ports, and power taps into the keyboard connector for these multiple devices that required sustaining a daisy chain of PS and AT male-female and DIN-pin keyboard adapters. It is still too hard, even for a very technically savvy person, such as I see myself, to install, integrate, and access quirky web sites.

The bottom line is that I explored these input devices. It is important to know that the intent of the :CueCat is to provide special oblique barcodes in catalogs and in magazines that a reader, when a reader scans an "advotorial" barcode with the :CueCat, opens a supplemental web page with technical details, pricing, and the usual puffery. Most often, I was shown a blank under construction page… not a very good result. The AMEX magnetic and smart card reader is intended to provide secure Internet ecommerce purchasing on the web. They represent primitive solutions with limited abilities. I think these implementations will be dead soon.

However, the exploration took an unexpected turn to highlight a bigger picture with serious securty ramifications. No matter how we advance security, we undermine it. Specifically, Linux users voiced unhappiness at a lack of :CueCat support from Digital Convergence, its manufacturer. As a result, a number of open source Linux programmers created a flood of :CueCat drivers for Linux and ported the URL activation code into Java scripts. Although Digital Convergence was disturbed about this loss of control, loss of quality control, and the potential for direct niche competition, that basic situation rapidly spun further out of control. Once open source code existed for the barcode scanner, other programmers modified the code to output the results of the interpretation of the barcodes and stuff it into the keyboard buffer, clipboard, or standard I/O streams.

Other programmers enhanced the code so that it now will read any and all of the 30 or so different industry-standard barcode fonts, not just the specialized oblique Digital Convergence barcode. Companies like Zebra and Worthington must be unhappy that there is a now effectively a free barcode scanner on the market. But that is not the issue either. The Linux drivers have been ported to Microsoft Windows; I even have Visual Basic, C++, Java, and Perl component code to read barcodes with the :CueCat. The original intent has been subverted. Some market niches have been jeopardized and some business methods have been made irrelevant and exposed to others to exploit in new and different ways—direct competition with Digital Convergence. The barcode scanner is not a security device, but the story does get worse.

The AMEX card reader is a security device. It is intended as such. It is sourced from Gemplus, a manufacturer that sells different types of card devices and software development kits. The labels on the packaging and on the device itself opens a Pandora of technical information and opportunity. I located a complete software development kit on the Internet (from a so-called WAREZ site where commercial software is pirated). I also traced some interested threads with return addresses at major financial and software development companies explaining card writer hardware and software, and in particular ways to reapply the AMEX reader. As with the :CueCat bar code, the original intent of the AMEX smart card reader has been subverted. For example, there is a lively discussion thread on the Usenet mail group, ALT.HACK.DSS, focused on how to use the free AMEX card reader to alter DSS satellite dish receiver access cards (for Dish, DirectTV, Hughes, etc.) in order to get all the subscription channels (some 500 of them).

The AMEX card reader and the Blue program were designed in reaction to the failure of the SET (Secure Electronic Transactions) protocol programs at MasterCard and Visa. These programs were designed to decrease fraud levels for the card issuers and clearinghouses. The merchants were, and still are, the primary "beneficiaries" of credit card fraud, and in no way protected by SET. The slowness and complexity of SET has doomed it. The AMEX Blue program is partially designed to help the merchants. However, the other stakeholder in the credit card market is the cardholder. Cardholders are already indemnified to a maximum loss of $50 for fraud (at least in the US), and most card issuers write off all fraud as a matter of practice. Cardholders thus receive no financial benefit from the AMEX program other than this free handy-dandy high-tech dongle for their computers that they can brag about.

As an aside, some issuers already set responsibility limits to $0, such as AT&T International Card, so cardholders receive like benefits with fewer workflow complications and computer installation headaches. My assessment is that the Blue program is basically an expensive marketing campaign with questionable tactics and minimal possibility for long-term survival. It has been incredibly effective at cannibalizing market share from MasterCard and Visa, because the lack of real financial rewards means that an aggressive campaign by these competitors with similarly useless reward premiums will recover fickle cardholders. Imagine if a credit card issuer actually creates a valuable and novel reward program, such as the Shell MasterCard 5% gas rebate and 1% purchase program to compete against the tiered ¼% and ½% DiscoverCard kickback program. AMEX Blue seems like a knee-jerk reaction to Internet E-commerce at best to me.

Nevertheless, the story gets worse. This is not about cannibalization, vacuous marketing campaigns, and silly attempts to enter the ecommerce market; it is about the abject failure of barrier security. Let's focus on security. The proposed reason for the card reader is to authenticate the user and the card by name, login, password, credit card number, and location at time of online purchase. The magnetic stripe and the embedded computer chip provide a locked door and a deadbolt, so-to-speak. Apply the situation of :CueCat reader exposure to a comparable exposure with the AMEX Smart Card Reader and the loss of control becomes a serious undermining of the present security infrastructure.

Specifically, a free device makes it possible to read credit cards with magnetic stripes, ATM cards, debit cards, and other ID cards. If you do not see that, read this again. This is really serious. It is not the fault of American Express, it is just the manifest destiny of the proliferation from any sufficiently advanced technology. The Smart Card is a reader for any ID-1, the standard credit card as defined in ISO/IEC 7810, and by the way, also a writer, since the same device reads and writes to the Smart Chip despite AMEX and Gemplus assertions to the contrary. Add to this atomic bomb, complete cookbook instructions to apply and obtain other smart chip writers with software for $74 USD from the ALT.HACK.DSS and other newsgroup chatter. Exposure is really cheap without even registering with AMEX.

So now you see the risk of a community with the ability to fully read magnetic stripes, write, recode, and alter various ID and financial service cards, not just the American Express Blue cards but any financial card with a smart chip. However, the story gets worse than that. There is more systematic risk through the reverse engineering of the Blue Internet ecommerce process. Anytime, anywhere, against any merchant, with randomly constructed credit card numbers, a criminal intent on fraud will be able to buy products online, potentially move money through EFT with the new Private Party payment service, or simply counterfeit transactions for payment, refunds, or chargebacks. The new technology coupled with the inherent complexity and distributed nature of the e-commerce infrastructure increases the risk portfolio for massive fraud for all players.

Given the scope of this catastrophe, this is still not the end of the story. If we extrapolate the process, all security and biometric workflows can be reversed engineered, attacked within the context of a distributed transaction processing environment. Not only are the public Internet, VPN, and private channel distribution grids at risk from snooping and interception as we all know it, the security hardware and interfaces we expect to be secure represent open and accessible points of attack. The result is that security is a no-win battle of building bigger and stronger fortresses with built-in obsolescence. Within the open source code movement, the online hacker's galleries, the free flow of protected speech in the newsgroups, all at Internet speed, the period until obsolescence is decreasing from the traditional 18 months, to two months in the case of the :CueCat, to just under 2 days in the case of the American Express Blue Smart Card Reader. Although there might not as of yet be frauds committed with Blue or other financial cards, this is merely a matter of time. The stage is clearly set and the siege technology is fully in place to win against all security barriers. The barriers to entry are none, $74 at most in the AMEX example to read and write magnetic stripes and smart chips embedded in all types of standard plastic security cards.

Even traditional encryption methods contain seeds for its own defeat because the infrastructure provides tools, information, distributed power, and combined resources to penetrate any walls. The promises and threats from quantum computing, the next foreseeable leap in technology, contain both hope but also the tools to defeat encryption. Even there, the barriers to entry are likely to be short-lived.

The bottom line is that security technology based on moats, walls, firewalls, Marginot lines, submarine nets, mine fields, or other types of physical and logical barriers is obsolete and ineffective. The time frames for siege-based penetration to succeed is reduced to mere hours. The time for the protection of any moat to fall to the effort of skilled "professionals" is moot. (Sorry could not resist the word play.) These protections are effective only against the morally righteous customer, vendor, business partner, or workflow ally, not against the concerted, aggressive, and motivated attacker. Consider also that the metaphor of the protective wall is designed against the two-dimensional attack. It readily fails against three-dimensional attacks mounted by terrorists, moles, insiders (that might even belong to your own organization), excavators, paratroopers, those granted permission to pass through the walls, and even those perpetrating a physical and social Trojan Horse strategy. Barriers are too obvious and too permeable. As to what is better, stay tuned. I will let you know. The US government is losing the battle. Microsoft cannot keep source code thefts at bay, and Cisco seems to be a hot target. If you paint a bull's eye, some people want to prove that they can find it.