Electronic Banking Security
RUSSELL J. DAVIS

Strategically located throughout the FDIC are pictures depicting the consequences to banks of the ’29 stock crash. To recognize the importance of consumer confidence, one need only recall the newsreels showing the hollow faces standing in line to withdraw their bank funds. Perhaps the most important service we offer is consumer confidence at FDIC insured institutions. This confidence must be preserved in light of ever changing technology.

Typically, improved controls are applied only after a significant loss. For example, the Rifkin Fed Wire transfer scam that precipitated tighter security controls being applied to Fed Wire. Today, we would look at the controls in place then as being inadequate. An evolving challenge is to predict what controls can be applied that will mitigate exposure.

With the advent of automatic teller machines, banks discovered a cheaper, faster, and arguably better method for providing service to customers. Since their inception, additional controls, such as security cameras were deemed necessary. Still, the ATM model has proved successful, in part because users are required to access a physically controlled ATM machine, possess a valid ATM card, and must know the personal identification number (a.k.a., a PIN or password). Compare this with the losses incurred due to credit card fraud. Many of us know people who have had a credit card used for fraudulent purchases. But how many people know of a person victimized using the ATM?

So how do credit cards and ATM cards differ? In general, the mere presenting of a credit card to a vendor is usually enough to authenticate a transaction, without requiring additional information from a customer. But two separate and distinct steps (possession of the card and a valid PIN) are required to validate an ATM card transaction.

These examples should give you some idea of the challenges that confront the electronic banking initiatives currently underway. For electronic banking, the first significant difference is the media that information traverses. In the case of credit cards, the store typically uses a phone connection to transfer information. With electronic banking, the Internet is typically used to communicate information. **Robert T. Morris Jr.**, demonstrated to the world just how connected (and vulnerable) the Internet was back in 1988. Late that year, he released the infamous “Morris Virus” (a.k.a. “Morris Worm”) onto the Internet. Within hours, the Internet was on its knees. Although the vulnerabilities used in the attack were widely known, there was no serious effort to plug the holes until after the fact.

Unlike the ATM that is physically controlled and the credit card reader that is located in the store, the electronic banking consumer’s home computer is outside the control of the bank. The home computer, along with the user’s internet connection, provides an alternative path into consumer bank assets. There is currently no control on how consumers use their computers at home. The potential for significant loss could be incurred during a simultaneous attack. That is, as the number of successful attacks occur, the greater the likelihood for bank insolvency. This is the electronic equivalent of a large number of depositors standing in line to withdraw their funds.

A significant difference is the electronic example can take place in a very short period of time (perhaps measured in seconds).

With the potential for significant losses, it is in our best interest to be proactive in understanding how we can limit the risk. Obviously, banks should look out for large funds transfers occurring over a short period of time. Additionally, products with better security controls could mitigate potential losses. It is now appropriate to give an example of controls being applied to an emerging application.

References:

Echin, M. W. and Rochlis, J. A. , *With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988*, Communications of the ACM, June, 1989.

Greguras, Fred, *Corporate EFT: Vulnerabilities and Other Audit Considerations*, IPC Business Press Volume 3, Number 3, May, 1981.

Yang, Yi-Jen, *The Security of Electronic Banking*, Proceedings of the 20th National Information Systems Security Conference, pages 41-52, October, 1997