SAND97-1335C

CONF-9706109--5

Threats to Financial System Security

Douglas E. McGovern, Ph.D.
Sandia National Laboratories*, Albuquerque, New Mexico
Phone: (505) 844-1542

Abstract

The financial system in the United States is slowly migrating from the bricks and mortar of banks on the city square to branch banks, ATM's, and now direct linkage through computers to the home. Much work has been devoted to the security problems inherent in protecting property and people. The impact of attacks on the information aspects of the financial system has, however, received less attention. Awareness is raised through publicized events such as the junk bond fraud perpetrated by Milken or gross mismanagement in the failure of the Barings Bank through unsupervised trading activities by Leeson in Singapore. These events, although seemingly large (financial losses may be on the order of several billion dollars), are but small contributors to the estimated $114 billion loss to all types of financial fraud in 1993. Most of the losses can be traced to the contribution of many small attacks perpetrated against a variety of vulnerable components and systems. This paper explores the magnitude of these financial system losses and identifies new areas for security to be applied to high consequence events.

Introduction

In the study of high consequence security related events, anticipated losses can be very large. The anticipated probability of occurrence is, however, very low and data describing the history and potentialities is limited. The opposite holds true in the financial world. Total losses are large but the typical individual loss is limited to a fairly small contribution. The number of events, however, is large enough to allow reasonable tracking of some of the costs, estimation of likelihood, and understanding of the actions. Most of these events derive from malevolent intent. As the world-wide financial system transfers more of its value through "megabyte money" and less through exchange of pieces of paper, the areas of vulnerability (and the associated potential losses) change. This paper discusses the present state of the world, both in consideration of the volume of legitimate transactions and values and the impact of fraud and theft. New threats are identified in the information world which have the potential for significant future losses.

HH

---

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

DISCLAIMER

Description of the System

Information Quality

The information presented below is obtained from multiple sources. Some information is repetitive, some is overlapping, and some of the sources are not considered highly reliable. The aggregation of this information does, however, provide an "order of magnitude" picture of the financial system and the associated high cumulative consequence due to multiple events.

Financial Systems

The world financial system supports the storage, collection, transfer, and handling of financial value through a variety of institutions. These institutions include not only banks and lending agencies, but debit and credit card companies, firms that provide for the collection and transfer of currency, organizations supporting the financial system through the issuance and control of stocks and bonds, trading organizations, regulatory bodies, etc. There is also an associated service industry providing manpower, computer hardware and software support, security, service analysis, and other activities necessary to keep the entire conglomeration of functions operating smoothly. The items of commerce may be coins or currency, stock certificates, wire transfer receipts, other types of paper instruments, or may be strings of digits in electronic form.

There are thousands of banks of many sizes in the US. A large regional bank is one with $10-25 billion in assets. A super-regional bank has assets between $25 billion and $75 billion. Mega banks are those with assets in excess of $75 billion. To sustain commerce, banks handle 60 billion paper checks per year. In fact, at any one time, there may be over 11 billion pieces of paper in process in the US banking system.

The Nilson report estimated that, in 1995, the US "pay-before" transactions (cash, traveler's checks, money orders, etc.) constituted an $800 billion market. "Pay-now" (personal checks, electronic funds transfer at the point of sale and automatic account debiting) were a $2,200 billion market. "Pay-later" (credit cards, charge cards, etc.) were over $650 billion. It is interesting to note that 85% of US payments are made in cash but these payments represent only about 1% of the value being exchanged, while the 2% of payments utilizing electronic funds transfer account for 85% of the value.

Worldwide cash transactions (coin and currency) are estimated to be worth in excess of $8,000 billion per year.

Interbank transfer of funds is required for transaction settlement. Hitachi estimates that this global interbank market is in the range of $4,000 - 5,000 billion per day. In the US alone, the major networks (CHIPS and Fedwire) handle over $2,000 billion per day. Note that this corresponds to one US Gross Domestic Product every 2.5 days.

Credit Card Management Magazine (May, 1995) estimates the US credit card charge volume to be over $580 billion in 1994 (including Visa, MasterCard, American Express, and Discover). This is nearly 50% of the over $1,200 billion 1994 estimated world volume. The overall growth rate in credit card transactions is in excess of 20% per year. MasterCard alone licenses approximately 12 million terminals around the world to support this market. In Canada (as of October, 1996), MasterCard and Visa together supported 30 million cards in circulation with an average sale of $77 but a net retail volume of over $67 million.

There are over 210 million on-line debit cards in use in the US today.

The value of all stocks on the New York Stock Exchange exceeded $5,000 billion in 1995.

Smart Cards (credit card sized cards with onboard integrated circuitry) are rapidly becoming a preferred mechanism for such things as prepaid phone cards, intelligent credit cards allowing off-line transactions, and stored value cards (the electronic purse). While just beginning to make an impact in the US, smart cards are very common in Europe and the rest of the world. SGS-Thompson, one of the manufacturers of the integrated circuits used in smart cards announced that late in 1995, they had shipped their 1 billionth integrated circuit for smart cards. Gemplus (one of the major suppliers of assembled cards) shipped their 500 millionth smart phone card in October of 1995. In fact, Gemplus estimates a world market exceeding 3.8 billion cards by the turn of the century. As will be discussed later, smart cards not only provide for new mechanisms for commerce, they allow on-board encryption for enhancing the data security.

Numerous other statistics supporting the overall size of the financial market could be cited but the above should suffice to indicate the very large volume of wealth which is being manipulated twenty-four hours a day, every day of the year.

Magnitude of the Problem

It is estimated that $114 billion was lost in the US due to fraud and theft in 1993. At the present growth rate, losses in excess of $200 billion per year can be expected at the turn of the century. As an example, Nick Leeson caused the $1.4 Billion collapse of 232-years-old Barings Bank through improper trading, primarily on the Singapore International Money Exchange. This problem is very widespread as found by a major survey of 2000 large corporations in which 77% reported at least one instance of fraud per year.

Attacks against the physical manifestations of financial institutions are very old attempts to illicitly gather wealth or power. As Willie Sutton so eloquently put it when asked why he robbed banks : "That's where the money is." The traditional attack entails physical compromise of some part of the system through a covert penetration or an overt attack (armed robbery) leading to removal of negotiable instruments. Planning, preparation, or the attack itself may be aided or abetted by an insider. Bank robberies, mail theft, train

robberies, diverting deliveries at airports, etc., are all examples of this traditional attack. In 1994, the FBI reported over 7,500 bank robberies with losses of $68 million.

Other forms of fraud include forgery, counterfeiting, generating and passing worthless checks, etc. For example, more than 1.2 million worthless checks enter the banking system each day. Check fraud was estimated to be between $3 billion and $10 billion in 1993. Note that bank robberies are more publicized but represent just a fraction of this loss.

As reported in US News and World Report (December 5, 1994) it is estimated that there is over $10 billion of counterfeit American currency in circulation outside of the US.

Credit card losses (worldwide) average between 7 and 15 cents per $100 charged. Given the size of the market, this represents a world wide loss of between $800 million and $1.8 billion for credit cards alone. Visa reports more than $350 million fraud loss in the US for the four quarters ending September 30, 1994. The vast majority of this is from lost, stolen or counterfeit cards. The average fraudulent transaction is between $100 and $200 and is one of typically five transactions before the account is closed.

One man, Kenneth Steven John, has been found to have 45 distinct identities, supported by 61 driver's licenses issued by 6 different states. This would be just a curiosity except that, as a result of his multiple identities, he accumulated a net worth in excess of half a million dollars through credit card scams and check kiting.

Even such mundane items as parking meters are not immune to loss. In 1995, the city of Vancouver lost $500,000 to theft and damaged equipment.

In Japan, Pachinko parlors provide patrons the opportunity to play a form of pinball with the incentive of minor gambling. The customer can pay to play using cash or prepaid Pachinko cards. In April, 1996, 52,000 fake Pachinko cards were seized.

The advent of new services has provided new opportunities for fraud. Credit and debit cards have provided means for transfer of value by consumers via strings of numbers. These could be transmitted over the telephone, through dedicated networks, by mail, or in person at points of sale. Electronic funds transfer, either at the major bank level or through home banking, provides another example of value represented by digital strings. Electronic cash and business over the Internet are extreme examples. Diversion of funds, gathering of information, and modification of transactions are all possible through electronic connections or by hacking into data processing. No physical contact, penetration, or possession is required. It is these type of attacks which hold the potential for the greatest present and future levels of fraud. When people speak of electronic commerce, the vision is the internet equivalent of an air-conditioned, security conscious mall with convenient parking, well behaved shopkeepers and multiple methods of payment. At present the reality is closer to an electronic casbah. Let the buyer beware!

Citibank was attacked through a computer hacking attempt to transfer $12 million from its corporate cash management system to foreign accounts. Almost all of the money has been recovered.

The FBI, as reported by the Kansas City Star on February 10, 1996, arrested a salesman for computer crime. The alleged perpetrator had tapped into a former employer's voice mail system, causing an estimated $1 million in lost business. In another case, a former employee hacked a company's e-mail system, creating a complete mirror site. Messages were redirected to unauthorized employees and to competitors.

The European satellite TV system utilizes smart cards to provide the de-scrambling of signals for legitimate subscribers. The sale of cloned cards, hacked systems, and other types of piracy has become a $500 million per year business. The level of hacking has become so widespread that it is imputed that the larger pirate organizations are anxiously awaiting the arrival of an upgraded system so that the competition will decrease and they can begin making money again.

The band U-2 had their Dublin studio hacked, losing electronic copies of 2 unreleased songs. These songs became available on the black market months before the band had planned a commercial release.

Sources of Fraud

Criminals, including both outsiders and insiders, represent the largest threat for financial system loss. Actions are typically aimed at monetary gain, although sabotage or a desire for revenge against the system may be factors. The attack can be initiated from many different starting points. For example, Fraudwatch (First Quarter, 1996) reports on a psychotherapist that is being charged with insider trading from information revealed to him by a client during therapy.

Hackers, as indicated above, are a significant threat to the electronic handling of money and information. In many cases there is undeniable malevolent intent. However, hacking represents a potentially new type of threat with a motive based more on challenge and curiosity than on expectation of monetary gain. This is a growing threat as a result of proliferation not only of targets, but of capability openly available in the world community. For example, in 1991, more money was spent on hardware and software for information handling than was spent for production of hard goods. In the 2nd quarter of 1994, more computers were sold than television sets. As of the first Quarter of 1997, over 20 million households were connected to Internet services.

Common methodologies employed by hackers include virus, trojan horses and logic bombs. Virus attacks are based on the injection of illicit software into the computer operating system. A virus can be relatively benign (as an indicator of penetration), can serve to pass information outside of "protected" systems, or can lead to irretrievable

loss of data or destruction of hardware. The National Computer Security Association monitors the status of viruses. At present there are more than 7,500 distinct viruses known. The doubling time is on the order of 8 1/2 months. It is estimated that over half of the more than one million computers functioning as internet hosts have had viral incursions.

Trojan horses and logic bombs are software attacks that depend on unauthorized or illicit code buried inside other software. The trojan horse can open to allow data modification, to pass information, or to perform some other type of penetration. A logic bomb can be set to operate at a specific time or under specific circumstances to deny service, destroy parts of a data base, etc. These code objects could be inserted in delivered code or could be injected at a later time. The impact can be immense.

The Defense Information Security Agency performed a test on the vulnerability of military computer systems. In that test, they found that over eighty percent of the systems checked could be penetrated. Ninety-six percent of the penetrations went undetected. Only about five percent of the detected intrusions were reported.

In April of 1996, a St. Louis teenager was identified as a major perpetrator of computer fraud. He was in possession of hundreds of passwords to corporate computer systems including those of defense contractors. He also had information from credit reporting computers, calling card numbers and credit card numbers.

USAF personnel penetrated the command and control systems of a US Navy ship at sea through the use of an internet linkage. This penetration, performed as part of an authorized test, could have ultimately allowed injection of spurious commands to the ship-board operational computers.

It was reported by Reuters (9/19/95) that hackers had tapped into a French navy computer system, gaining access to files containing acoustic signatures. Ships involved included both French and allied forces.

The Naval Post Graduate School at Monterey, California, was hacked into from overseas. The Command, Control, Communication, Computer and Intelligence Professional (C4I-Pro) Bulletin board was penetrated. Although this is an unclassified bulletin board, there was potential for loss of information, disruption of communications and denial of service.

An additional source of threat which is relatively new to the financial system is attacks with national or quasi-national sponsors. There have been many instances of fraud emanating from several specific locales, particularly Nigeria. Iran is reputed to be counterfeiting US currency. One of the largest suppliers of credit cards is China, and few are supplied to legitimate businesses. The Russian crime organizations, drug related criminal organizations in such countries as Columbia and Burma, and general societal decay in the Balkans, parts of Africa, and other areas all contribute to the

growing threat from major organized efforts to penetrate a country's financial system for monetary gain or to destabilize an enemy.

Responses to Loss

The primary, and most effective, prevention tactic (or, alternately, the first area to improve in the event of a loss) are structured checks and balances in the system operation. It is estimated that 59% of electronic funds transfer fraud is due to poor internal controls. In fact, 36% is estimated to be due to management actions, overriding the existing internal controls that do exist. Thus, the most direct actions involve review, improvement, and close monitoring of personnel and system controls.

Just as technology has created new opportunities for fraud, technology has also contributed an arsenal of weapons for use in combating fraud. Perhaps the most glamorous is the use of neural nets to monitor expenditures and card usage. The history of a specific credit card is input to the neural net system along with general usage patterns which indicate fraudulent use. The real-time transactions are then monitored by the neural net to identify suspicious transactions. The credit card authorities are then notified so that the transaction can be checked further or, if appropriate, disallowed.

An alternate method used to monitor spending is "scoring". Scoring was originally derived from the decision process for initial issue of credit cards. In scoring, a series of rules are consulted. The similarity of the transaction to each of the rule characteristics results in a numerical score. When the aggregated score exceeds a certain amount, the transaction is flagged for further review.

Encryption of data is an effective tool for reducing vulnerability in a variety of situations. With encryption, data can be kept private. Data can be "signed" to ensure that the data received is identical to that which was sent. Data can be tagged to provide non-repudiation of the source. Finally, data can be uniquely signed, guaranteeing the source. Any or all of these can be implemented at the cost of additional hardware, procedures for key dissemination, handling and storage, and operational procedures.

Biometrics (measurements of some unique aspect of the human requesting use of the system) can be included in critical transactions. At present, much of the control is provided by what is owned. That is, access to a system requires a physical key or card. Further control is generated by what is known; e.g., a personal identification number or pin. Biometrics provide the final link by establishing who you are.

The integrated circuits in smart cards provide the means to carry the information required to support encryption, biometrics, and additional data security and control.

Related Issues

The discussions above have centered primarily on financial issues although a few examples were drawn from other forms of information attack as well. There are other events which, if experienced in the financial system, could have very high consequences. General system failures, as in the 1991 switch failures in the New York area telephone system, could lead to significant shutdowns of markets or banking capability. In the telephone shutdown, several major airports on the east coast were closed when air traffic controllers lost vital data. When malevolent attack is included, as in the case of information warfare, events could include disruption or shut down of vital communication or national control systems.

Denial of service and significant harassment can also result from other individual actions such as the "spamming" of Rush Limbaugh. An attacker (disgruntled listener?) signed him onto hundreds of internet e-mail lists, leading to total overload and shut-down of his capability to receive e-mail. (Within thirty seconds of emptying his e-mail in-box, the in-box was again overloaded and shut down.) A "cancelbot" wiped 25,000 messages from an Internet bulletin board. A SYN flood attack prevented a major shopping service from dealing with customers on the Internet for more than 40 hours prior to Christmas, 1996. In all cases, these acts appeared to be the result of individuals.

Conclusions

A review of the above variety and magnitude of attacks emphasizes that in financial security, as in physical security, consideration must be given to the system. Both people and hardware are included. The overall system security is no stronger than the weakest link.

Financial system security requires rigorous use of cost/benefit analysis. Even though losses can be in the billions of dollars, if securing a credit card transaction costs more than about five cents, it is not a cost effective solution.

Financial system security no longer applies only to banks. The entire information infrastructure is placed at risk.