Computer System Vulnerabilities

by Dr. Frederick B. Cohen

Abstract

In this paper, we **very briefly** overview computer system vulnerabilities in large information intensive organizations. Most of the problems we introduce have feasible solutions, but relatively few systems or experts are available to implement those solutions.

1 Background

Al Brunetti asked me to overview IS vulnerabilities to a group of NYNEX managers in 20 minutes or less. That's what this paper is all about. If you are not seriously concerned about protection in your organization before you read this paper, you should be afterwards.

Unfortunately, in only 20 minutes, I can't even hope to cover the well known vulnerabilities in the most secure general purpose computer system on the market, and since I've already wasted 30 seconds on the introduction, I'd better keep moving. Instead of trying to be exhaustive, I will try to deliniate the nature and scope of the problem, and give a few real-world examples to keep things grounded in reality.

For the purposes of this paper, I'll classify vulnerabilities in terms of organizational impact. I usually look at 4 general areas:

- Corruption: The inability to maintain standards of accuracy, or suitability. Systems that protect against corruption maintain 'integrity'.
- Leakage: The inability to keep confidential information in confidence. Systems that protect against leakage provide 'secrecy' or 'privacy'.
- Denial: The inability to provide expected services. Systems that protect against denial provide 'availability'.
- Evasion: The inability to accurately characterize what takes place. Systems that are able to accurately characterize what takes place have 'accountability'.

2 Curruption

The major impact of corruption is that we cannot trust the information we have to fulfill its purpose. For example, if a data entry clerk with dislexya entered the mailing lists used for client billing, we would presumably get numerous incorrect zip codes, and our monthly billing would come back largely undeliverable. This could result in a dramatic impact on cash flow, poor relations with the post office, and substantial costs for repairing the database.

A simple cure for this problem is the use of the postal database at data entry and output time to check and correct names, addresses, zip codes, and other data to meet the standard postal mailing address, but of course this is not the only sort of corruption we encounter.

One of the major problems with corruption is that most modern computer systems don't have systematic protection in place against it. The old addage 'garbage-in garbage-out' seems to apply in most cases.

One of the most disconcerting types of corruption today is the computer virus. Viruses corrupt other programs so that they propogate the virus as well, and thus spread like a biological disease through computer systems and networks. Viruses can carry damaging code along with them, thus turning all of your programs into corrupting influences. Imagine a virus that looked for 5-digit numbers and randomized the second digit. Every program in your computer could corrupt zip codes every time they ran. So much for the postal database.

There are also legal impacts of corruption. For example, a credit bureau has a responsibility for the accuracy of stored information. If management does not act prudently to protect stored information, they may be personally liable for the impact of inaccuracies.

3 Leakage

The major impact of leakage is the loss of competitive edge. For example, an industrial spy can usually get a job as a computer operator at night. From this position, it is common to be able to read information on mainframes and file-servers. If the spy finds information on pending contracts and sells it to competitors who underbid you, or if the spy gets your customer list and demographics information and exploits it to increase market share, or if the spy gets technical data and uses it to produce competitive products, it can cost your company a great deal of money. It happened to IBM when a Japanese company stole technical data related to mainframes and manufactured competitive products. If it can happen to big blue, it can happen to you.

Protecting from leakage in most modern systems requires good access control, authentication systems, physical security, and protection management. If you do not have these things, you are almost certainly vulnerable to widespread leakage.

In information related businesses, privacy of client information may also be vital. By leaking confidential client information, you may risk legal action. If you have both leakage and integrity problems, you may face a defamation suit based on the leakage of incorrect and damaging information about clients. If prudent methods are not in place, managers may

have personal liability associated with this sort of leakage. The

4 Denial

The major impacts of denial are increased frustration and lost time. AT+T has had major denial incidents in the last few years, including the loss of about 50% of the telephone service in New York for a day due to a cut cable, and loss of 50% of its long distance service for 1/2 of a business day due to a replicating network protocol. According to one of my estimates, the second loss ended up costing over 100 Million dollars! Consider all of the 800 and 900 number calls that couldn't get through and all of the lost orders resulting from that!

Protecting from denial usually requires uninterruptable power supplies, good facilities design, a good and well tested disaster recovery plan, and designed-in redundancy. These are necessary, but not sufficient conditions for continuity of service. After all, AT+T had all of these to one extent or another.

The problem of denial is especially vital in information related businesses because of the extreme dependency on information systems. For example, one large telephone service center on the West coast with over 500 daytime telephone answering employees had a virus bring down their entire network. I was called at 4AM because by 8AM, there would likely be over 500 calls per minute lost and over 500 employees sitting idle. Even at only US$10/hr for employee costs (a vast underestimate), that comes to US$5,000 per hour. If you include lost orders from businesses relying on the service and lost 800 and 900 number billings, totals can easily exceed US$500,000 per hour. We got them back up by 8AM (their time), but if they hadn't been able to get in touch with an expert at 4AM, they would have been up the proverbial creek without a paddle.

5 Evasion

Evasion takes many forms. One of the least understood issues in evasion is that without good accountability, you can't tell how much you're losing.

One of the best examples of this problem is the large number of people who ask me how much it will save them to have access control on their PCs. I generally respond that without any access controls and accounting, they can't tell me how much they are losing, so I can't

tell how much they could save; but with decent access controls, attackers don't get past the front door, so I also cannot tell them how much they are saving once they put these controls in place, because they are so effective. What I end up doing is telling them to use 'exposure analysis' rather than 'risk analysis', but I'll get to that (briefly) a little later.

Another example of evasion is the evasion of responsibility for attacks due to a lack of sufficient legal notice. In some states (New York is an example I believe), you are required to notify an attacker of the fact that a system contains proprietary information and is for authorized use only in order to pursue legal recourse on civil matters. This is normally the case for Trade Secrets, which comprise the vast majority of the information value in most current organziations. Is your customer information copyrighted or patented? No, it's a trade secret. The same is true for your bids, contracts, employee information, business methods, future products and services, marketing plans, allocation of resources, and almost all other business related information. If attackers can evade responsibility for their attacks, there is little motivation for them to stop attacking.

6 Interactions

In the information protection community, we often list issues separately, but they are really very closely intertwined, so that corruption often results in evasion, denial, and/or leakage, etc. Let me give you some good examples.

It is commonplace for computer virus defenses to look for known viruses but provide no access controls. Unfortunately, without any access control, 'stealth' viruses infect the defenses and cause them to miss the attack, and even worse, to infect all of the files as they are scanned at system startup! On the other hand, access control alone doesn't stop computer viruses either. The early experiments with computer viruses showed that they took over a typical timesharing system in only 1/2 hour, even with good access controls in place! In other words, to be effective, you must have both integrity and access control.

Even with good access controls and integrity protection, you need accountability for long term effectiveness. For example, given enough time to launch attacks, an attacker will eventually guess a password, steal an authentication device, attach to a dial-in line before it has completed the hangup procedure, or some such thing. In order to defend against persistent attack, we need to be able to detect the attacker's attempts to violate protection before they succeed. If we do this, we can detect and eliminate the source of attack before it is very successful. On the other hand, without access control and integrity protection, we can't get reliable accounting information, so accountability cannot exist in a vacuum either.

Finally, denial cannot be prevented if we cannot protect from arbitrary corruption of software, and similarly, without availability we cannot assure integrity or use our systems for their intended purpose.

Protection is synergistic in nature, and without comprehensive protection, we cannot effectively detect, prevent, or correct attacks. A chain is only as strong as its weakest link.

6.1 Summary, Conclusions, What Next

We have briefly touched on vulnerabilities, listed 4 issues to be examined; corruption, leakage, denial, and evasion; given examples of the impact of these issues, and discussed interactions.

We conclude that it's easy to lose a whole lot of money by not protecting your information assets, that it happens quite often, and that it happens even to the largest companies.

So what do you do about it? Buy my products! *(show products here)* But seriously ...

Rational protection decisions involve assessment of exposures, determination of costs associated with covering those exposures, and making judgements about whether the cost of coverage is justified.

The field of 'risk analysis' is based on assessing probabilities of events and expected losses from those events in an effort to determine expected loss; and assessing the change in those values associated with proposed coverage. In this case, the 'probability', 'expected loss', 'events', and 'change in those values' are the judgements made on the basis of experience. Arithmetic is provided to legitimize the activity.

An alternative is 'exposure analysis' in which we scare ourselves out of complacency by determining worst case losses, and provide some amount of coverage for the more severe exposures. But perhaps this discussion is better suited to our afternoon workshop.

I hope that I have provided some insight into the nature and scope of vulnerabilities, and that I have provided enough entertainment to keep you awake enough to get the message. But just in case, let me make my point again.

Information systems are like two edged swords. They are very potent weapons, but if you're not careful, you get cut.