INTRODUCTION

Research papers generally treat the problem of computer security as an intentional act to be solved by intellectually challenging methods such as encryption, descriptor-based systems, and program proving. Accidental and intentional acts are almost always referred to simultaneously; however, the safeguards are designed strictly to prevent intentional acts. It is generally thought that the same safeguards and strategies will be effective against both accidental and intentional acts. This is not necessarily true.

In a paper on security assessment by Glaseman, Tum and Gaines, accidental and intentional differences are not stated but are made subservient to the question of exploitation of vulnerabilities. As with most research papers on security, important research issues are discussed but they are oriented principally to intentional acts. This is evident in use of terms such as "intruder," "attacks," and "exploit," but no discussion penetrates research needs for errors, omissions and other accidents.

In contrast, Courtney states in a paper on risk assessment:

"It is important that proper weight be given to the impact of errors and omissions. Data is more often destroyed or otherwise rendered useless or even harmful by people making mistakes than through dishonesty or malice. People whose loyalty and honesty are unquestioned but whose judgment and competence leave much to be desired are our greatest enemies. Data security consideration must not be limited to concern for the acts of dishonest people. Otherwise, it is very difficult to achieve proper cost justification of appropriate security measures. Weigh all potential security problems... The differences between accidentally and intentionally caused losses are many and profound."

Unfortunately, he does not pursue these strong position statements to exploit the differences.

CHARACTERISTICS OF ACCIDENTAL AND INTENTIONAL ACTS

Frequency

Incidence of errors and omissions is usually sufficiently high to support statistical analysis of loss cases in a computer service organization. A limited number of cases, however, is often tolerated because the expense of reducing incidence any further is not cost-effective. Analysis can be used to identify the major locations and sources of errors and omissions. Statistics on the incidence of accidents can be used to calculate the probability and expected loss from these problems.

Conversely, the low incidence of intentionally caused losses makes statistical analysis difficult. Only in limited cases, such as credit card and some other payment frauds, has the incidence been high enough to be subject to statistical analysis. Most intentional acts, especially those involving significant losses, occur so infrequently that attempts to calculate probability, expected loss, nature, patterns of location, and source, are difficult if not impossible. Therefore, risk analysis at the present time must be more subjective and theoretical. The experience of victims that could be similar to experiences of future or potential
victims may be helpful in calculating statistical probabilities, but will probably not be sufficient.

Unsolved problems

There are few unsolved problems with regard to accidentally caused losses. Efforts to control unintentional losses have been made throughout the development of electronic data processing. Adequate solutions are known for most common errors and omissions. The causes of errors and omissions are mostly obvious and the solutions equally obvious. It remains to apply these solutions in a cost-effective manner. Nonetheless, despite the errors, computer operating systems, for example, are still effective.

In contrast, significant problems in security against intentionally caused losses remain unsolved. The technical security of currently available computer systems is inadequate against attacks from potential perpetrators (such as systems programmers) with sufficient skills, knowledge, and access to the systems. Moreover, computer operating systems are basically unpredictable. Therefore, proving the integrity of a system and guaranteeing freedom from unauthorized changes or enhancements are not possible at this time. Neither practical prevention nor adequate detection capabilities are currently known for such sophisticated attacks as Trojan Horse methods, salami techniques, data leakage, logic bombs, asynchronous attacks, or post system failure attacks. Another problem yet to be solved is the adequate identification verification of legitimate remote system users. Where technical safeguards are inadequate, therefore, more difficult and costly methods of safeguarding must be developed for protection from intentional acts.

Act complexity

Accidentally caused losses derive from single, isolated acts. Each loss incident is usually independent of other loss incidents. On the other hand, an intentionally caused loss can result from sequences of dependent and independent authorized and unauthorized acts. The loss can occur from intentional efforts that capitalize on observed errors and omissions. Perpetrators often increase the complexity of intentional acts as a means of avoiding detection or apprehension.

Singularity of source

One person usually is responsible for an error or omission even though other people may cause extenuations, whereas more than one individual frequently perpetrates an intentional act. Half the known cases of computer abuse have involved collusion. Compared to manual, or non-computer related fraud, embezzlement, etc., there is much more collusion in perpetrating these crimes via computer. The reason for the high degree of collusion is that computer crime requires more skills, knowledge, access, time or resources than any one person usually possesses in the technically oriented environments of the computer systems. Security strategies and safeguards must be far more elaborate when one attempts to deal with the possibility of collusion.

Complexity of perpetrator behavior

Behavior of people causing errors and omissions is relatively simple. The behavior is related to the conditions at the instant of the act. After the act, the perpetrator need, at most, defend only his weakness that resulted in error. In contrast, the behavior of people performing intentional acts is often highly complex. Interviews with 23 people who intentionally perpetrated a computer crime revealed that these people had personal problems to solve or goals to reach preceding their search for vulnerabilities of a computer system or work environment. Searching or studying a system for vulnerabilities is, however, only one facet of the complex behavior pattern of intentional perpetrators. Once motivated to penetrate and use a system to his own ends, a perpetrator plans, plots, gathers information, organizes, and conspires, and is left finally to rationalize all of his intentional acts. Effective security must address all of these issues.

Sources of security assistance

Accidentally caused losses have been extensively studied and reported in the technical literature for many years. As stated previously, however, most technical literature that claims to address both accidental and intentional acts effectively addresses only accidentally caused losses. Professional societies and governmental organizations dedicated to the prevention of intentionally caused losses have only recently attempted to examine the problems associated with computer technology. The American Society for Industrial Security, the U.S. Justice Department, the International Association of Chiefs of Police, National Crime Prevention Association, and Surety Association of America have barely, if at all, seriously or significantly addressed the criminal aspects of computer usage.

Security checklists

Much security literature relies heavily on checklist or cookbook approaches to computer security. Strategy is based on the concept of implementing the well-known safeguards and controls identified in the checklists. Although this approach is particularly effective for handling errors and omissions, it is neither sufficient nor effective in dealing with intentionally caused losses. Perpetrators are aware of the safeguards and controls identified in checklists, thus their methods for compromising the system are designed to avoid them. Merely installing a named safeguard in a checklist is not necessarily sufficient protection from intentional acts. Moreover, the checklist rarely includes information
Concerning the need and means of protecting the safeguard itself from attack or compromise.

**Strategy and safeguard independence**

Each error or omission possibility can be effectively treated in isolated ways, because one loss will be independent from any other loss. Thus, a safeguard against an accidental loss can be implemented without considering other possible losses. Basically, the formula of matching one error with one safeguard is reliable.

On the other hand, each intentionally caused loss possibility must be covered comprehensively, including all possible acts leading to the loss. A safeguard against an intentional act will often have impact on other types of acts or losses in that it may only partially supply adequate protection. A particular loss could result in a security strategy involving many safeguards or a defensive depth of multiple rings of safeguards which may be a desirable strategy. Further, the implications of imposing a safeguard must be considered in terms of its potential to open new possibilities of vulnerabilities. If a particular safeguard temporarily deters a perpetrator, he will simply seek ways around it or other vulnerabilities.

**Safeguard compromise**

In accidental loss situations, it can generally be assumed that the integrity of the safeguard will be ensured and sustained. Safeguards may be subject to failures from errors, but in general the errors will be independent of the errors that the safeguard is preventing. In contrast, safeguards are subject to intentional attack as part of the perpetrator's strategy in carrying out an intentional act. The compromise of safeguards becomes part of the total loss event that the safeguards are meant to prevent or detect. In this sense, a safeguard must be considered as an asset subject to protection if it is to perform adequately when needed.

**Level of protection**

Determining the level of protection that a safeguard from an accidental act affords is simple because of the one-for-one, act-safeguard relationship. Higher incidence of accidents can result in more easily calculated protection levels. In intentionally caused acts, the level of protection is determined by a combination of security measures associated with a given asset. Lack of statistics makes effectiveness difficult to determine.

**Achievable protection level**

Security from accidental losses can be achieved to a high degree or, at least, can be easily controlled at a wide range of loss levels. One reason for this is that the success of protection can be accurately measured from incidence statistics, and the security then can be changed on the basis of the need that is determined. Because there are few unsolved protection problems with accidental losses, it is possible to control incidents to any degree desired within the limits of economic considerations.

A high level of protection from intentionally caused losses is difficult to achieve because of incomplete knowledge of all vulnerabilities. An individual loss could be affected by many factors, including the difficult-to-determine completeness of protection. The one-upmanship escalation of protection and increasing sophistication of perpetrators' methods precludes reliable measurement.

**Potential perpetrators**

The population of potential perpetrators of accidental loss is easily identified. It consists of those persons having the access and authorization to perform an act that might result in an accidental loss. Conversely, the population of potential perpetrators of intentionally caused losses is difficult to identify. It includes not only those persons relative to accidentally caused losses, but also the often larger numbers of people who might gain the necessary skills, knowledge, and access to perform an unauthorized act. For example, in remote terminal usage, impersonation alone would account for a large number of people who might possess such skills to replace people in positions of trust.

**Potential perpetrator capabilities**

In accidentally caused losses, the minimum skills, knowledge, and resources of potential perpetrators are at issue. Access is a prerequisite. Beyond this, the security specialist is dealing with the minimum skills and knowledge of people that are the source of errors and omissions. With intentionally caused losses, the security specialist is dealing with people who potentially have the maximum possible skills, knowledge, access authorization, resources, and time to commit the act. The attack possibilities and matching protection activities constitute a game in which each side is pitting its maximum capabilities against the other side.

**Loss limits**

Accidentally caused losses are limited in size. Where the size of the loss can vary, the probability of detection and termination of the loss grows rapidly with the size of the loss. The victim is ordinarily able to observe, measure, and limit accidental losses in a timely manner. However, detection of intentionally caused losses in a timely manner is not necessarily related to the size of the loss. Exceptionally large losses can go undetected when the perpetrator puts forth significant effort to conceal the losses. Also, in increasingly automated criminal methods, the possibility of a large loss in a time scale measured in milliseconds before humans can react becomes more likely.
Detection

Perpetrators of accidentally caused losses have no conscious intention to err before and during their acts. Therefore, avoidance of detection occurs, if at all, after the act has occurred. There is generally less fear of detection or of reporting the loss and more cooperation with the victim in recovery in accidental loss situations as compared to the perpetrators' position relative to intentional acts. Interviews have revealed that perpetrators greatly fear unanticipated detection before, during, and after their acts, and often much of their efforts and resources go into prevention of detection. This makes detection of intentionally caused losses a much greater challenge than for accidentally caused losses and should occupy a greater amount of the security specialist's attention.

Theoretical approach

Support for claiming a difference in risk between accidental and intentional acts can be shown in mathematical terms, even though this procedure is highly theoretical and not intended for practical use. Given an asset subject to accidentally or intentionally caused loss, its environment, and a population of potential perpetrators with known skills, knowledge, access, resources, time and motivation. The probability $P$ of a particular type and size of loss $L$ from any possible independent accidental acts $a_i (i=1,2,\ldots,n)$ with probabilities of their occurrence $p(a_i)$ is $P(L) = \sum_i p(a_i) - \Pi_i p(a_i)$. This suggests that a safeguard that reduces the probability of an act $a_i$ for any value of $i$ will reduce $P(L)$.

The probability $P$ of a particular type and size of loss $L$ from any possible independent intentional acts $a_i (i=1,2,\ldots,n)$ with probabilities of their occurrence $p(a_i)$ is $P(L) = \max_i \{p(a_i)\}$. This conclusion is based on the theoretical premise that any potential perpetrator will perform rationally in choosing the act with the greatest probability of success. In addition, practical application of the theory implies that the population and all acts relative to loss of a particular asset are known.

Applying a strategy only for accidental prevention or only for intentional act prevention would clearly result in suboptimization, because many safeguards, some with minor modification, serve both purposes. A combined strategy, although not fully optimized, offers significant advantages over the near random-based, currently used strategies that are organized around merely computer center functional approaches (physical, operational, procedural and system) to security strategy. The steps to be followed in applying a combined strategy are:

1. Select the intentional act with largest probability of occurrence.
2. Apply safeguards to reduce the probability.
3. Identify the accidental acts also reduced in probability of occurrence.
4. Repeat Steps (1), (2), and (3) with the newly identified intentional act with largest probability until probability of intentionally caused loss is reduced to an acceptable level.
5. If the probability of accidentally caused loss is still not acceptably lowered, apply safeguards to reduce the probabilities of the combination of acts that reduce the probability of accidental loss to an acceptable level.

The alternatives of applying safeguards against accidental loss first or applying safeguards without regard to accidental or intentional act differences are less effective. Safeguards aimed only at accidental acts often will be ineffective or will not be the best safeguards against intentional acts. One reason for this is that the safeguards may be installed only against the compromise of assets and not with the intent of protecting the safeguards themselves against compromise. In addition, a particular order of implementation of safeguards may not be responsive to the strategies of the potential perpetrators who are looking for the simplest and safest route to achieving success.

Failure to use the recommended strategy results in the Maginot Line Syndrome: A monolith of obvious and traditional safeguards will be installed, and the perpetrator
merely bypasses it by finding the weakest link not yet addressed by the victim organization.

ILLUSTRATION

Implementation of access control by password to an online system from a terminal illustrates the problem. For purely accidental access prevention in a benign environment, identification verification by input of a minimal length password or name is all that is necessary. Prevention of intentional, unauthorized access to the system requires the following additional measures:

- Sufficient password length to reduce exhaustive search attempts.
- Assignment of randomly generated passwords to reduce guessing by analysis of dependence between password content and password holder characteristics or knowledge.
- Nonvisible input of passwords to avoid observation or scavenging.
- Frequent briefings of password holders concerning safekeeping of passwords.
- Safe password administration, including separation of duties; invocation of need-to-know principle; appropriate transport and storage of passwords; and specific authorization of duties to accountable and trusted employees to avoid spoofing, coercion, degradation of care, and unauthorized physical access attempts.
- Encryption of on-line system password files and password comparison in encrypted form in privileged mode computer operation to prevent technical compromise.
- Limit guessing attempts of unauthorized passwords by imposing time delays between input attempts and disconnect after $n$ failed attempts.
- Record and verify password use periodically with password users to avoid password theft and unauthorized use.
- Analyze patterns of password use and failed access attempts for deviations from normal experience to detect unanticipated attacks.
- Test all protection mechanisms frequently and prepare and follow contingency plans to avoid attacks when system or operational failures occur.
- Perform frequent, random, independent, and visible audits to inhibit potential perpetrators and ensure safeguard integrity.
- Impose sanctions against violators.

These additional safeguards are not new, but it is difficult to find them all stated in a single source. Again, subsets of them have been implemented, but are not generally found in a single computer service organization. For prevention of accidental access, only a few are needed. For prevention of intentional acts, all are needed; however, total implementation of all safeguards still is insufficient protection in many high-risk environments. Many more detailed specifications are needed for such items as levels of encryption effectiveness, pattern analysis of password use, password length, and audit techniques.

CONCLUSION

Glaseman, Turn and Gaines conclude by stating two major requirements for progress in security assessment:

1. Increased research aimed at the development of a better understanding of the informational elements of security assessment, and
2. Experience at the level of individual computer installations, in the application of a broader and more accurate information base to the assessment of computer security.

A third requirement should be appended to those suggested above:

Recognition and separate treatment of two separate and distinct computer security problems, accidentally caused losses and intentionally caused losses.

REFERENCES
