Computer Security and the Law

Gary S. Morris
GSM Associates
Suite 202
7338 Lee Highway
Falls Church, Virginia 22046
(703) 685-3021

Introduction

You are a computer administrator for a large manufacturing company. In the middle of a production run, all of the mainframes on a crucial network grind to a halt. Production is delayed costing your company hundreds of thousands of dollars. Upon investigating, you find that a virus was released into the network through a specific account. When you confront the owner of the account, he claims he neither wrote nor released the virus, but admits that he has distributed his password to “friends” who need ready access to his data files. Is he liable for the loss suffered by your company? In whole, or in part? And if in part, for how much? These and related questions are the subject of computer security law. The answers may vary depending on the state in which the crime was committed and the judge who presides at the trial. Computer security law is a new field, and the legal establishment has yet to reach broad agreement on many key issues. Even the meaning of such basic terms as “data” can be the subject of contention.

Advances in computer security law have been impeded by the reluctance on the part of lawyers and judges to grapple with the technical side of computer security issues [1]. This problem could be mitigated by involving technical computer security professionals in the development of computer security law and public policy. This article is meant to help bridge the gap between the technical and legal computer security communities by explaining key technical ideas behind computer security for lawyers and presenting some basic legal background for technical professionals.

The Technological Perspective

The Objectives of Computer Security

The principal objective of computer security is to protect and assure the confidentiality, integrity, and availability of automated information systems and the data they contain. Each of these terms has a precise meaning which is grounded in basic technical ideas about the flow of information in automated information systems.

Basic Concepts

There is a broad, top-level consensus regarding the meaning of most technical computer security concepts. This is partly because of government involvement in proposing, coordinating, and publishing the definitions of basic terms [2]. The meanings of the terms used in government directives and regulations are generally made to be consistent with past usage. This is not to say that there is no disagreement over definitions in the technical community. Rather, the range of such disagreement is much narrower than in the legal community. For example, there is presently no legal consensus on exactly what constitutes a computer [3].

The term used to establish the scope of computer security is “automated information system,” often abbreviated “AIS.” An AIS is any assembly of electronic equipment, hardware, software, and firmware configured to collect, create, communicate, disseminate, process, store, and control data or information. This includes numerous items beyond the central processing unit and associated random access memory, such as input/output devices (keyboards, printers, etc.)

Every AIS is used by subjects to act upon objects. A subject is any active entity that causes information to flow among passive entities called objects. For example, subject could be a person typing commands which transfer information from a keyboard (an object) to memory (another object), or a process running on the central processing unit that is sending information from a file (an object) to a printer (another object).

Confidentiality is roughly equivalent to privacy. If a subject circumvents confidentiality measures designed to prevent its access to an object, the object is said to be "compromised." Confidentiality is the most advanced area of computer security because the U.S. Department of Defense has invested heavily for many years to find ways to maintain the confidentiality of classified data in AIS [4]. This investment has produced the Department of Defense Trusted Computer System Evaluation Criteria [5], alternatively called the Orange Book after the color of its cover. The Orange Book is perhaps the single most authoritative document about protecting the confidentiality of data in classified AIS.

Integrity measures are meant to protect data from unauthorized modification. The integrity of an object can be assessed by comparing its current state to its original or intended state. An object which has been modified by a subject without proper authorization is said to be "corrupted." Technology for ensuring integrity has lagged behind that for confidentiality [4]. This is because the integrity problem has until recently been addressed by restricting access to AIS to trustworthy subjects. Today, the integrity threat is no longer tractable exclusively through access control. The desire for wide connectivity through networks and the increased use of commercial-off-the-shelf software has limited the degree to whichhmost AISs can trust its subjects. Work in integrity has been accelerating over the past few years, and will likely become as important a priority as confidentiality in the future.

Availability means having an AIS and its associated objects accessible and functional when needed by its user community. Attacks against availability are called denial of service attacks. For example, a subject may release a virus which absorbs so much processor time that the AIS becomes overloaded. This area is by far the least well developed of the three security properties, largely for technical reasons involving the formal verification of AIS designs [4]. Although such verification is not likely to become a practical reality for manyyears, techniques such as fault tolerance and software reliability are used to mitigate the effects of denial of service attacks.

Computer Security Requirements

The three security properties of confidentiality, integrity, and availability are achieved by labeling the subjects and objects in an AIS and regulating the flow of information between them according to a predetermined set of rules called a security policy. The security policy specifies which subject labels can access which object labels. For example, suppose you went shopping and had to present your driver's license to pick up some badges assigned to you at the entrance, each listing a brand name. The policy at this store is that you can only buy brand names listed on one of your badges. At the check-out line, the cashier compares the brand name of each object you want to buy with the names on your badges. If there's a match, she rings it up. But if you choose a brand name which doesn't appear on one of your badges, she puts it back on the shelf. You could be sneaky and alter a badge, or pretend to be your neighbor who has more badges than you, or find a clerk who will turn a blind eye. No doubt the store would employ a host of measures to prevent you from cheating. The same situation exists on secure computer systems. Security measures are employed to prevent illicit tampering with labels, positively identify subjects, and provide assurance that the security measures are doing the job correctly. A comprehensive list of minimal requirements to secure an AIS are presented in the Orange Book [5].

The Legal Perspective

Sources of Computer Law

The three branches of government, legislative, executive and judicial, produce quantities of computer law which are inveresly proportional to the amount of coordination needed for its enactment. The legislative branch, consisting of the Congress and fifty state legislatures, produce the smallest amount of law which is worded in the most general terms. For example, the Congress may pass a bill mandating that sensitive information in government computers must be protected. The executive branch, consisting of the Executive Office of the President and numerous agencies, issues regulations which implement the bills passed by legislatures. Thus, the Department of Commerce may issue regulations which establish criteria for determining when economic information is sensitive and describe how it must be protected. Finally, the judicial branch serves as an avenue of appeal and decides the meaning of the laws and regulations in specific cases. After the decisions are issued (and in some cases appealed) they are taken as the word of the law in legally similar situations.

Current Views on Computer Crime

Currently, there is no universal agreement in the legal community on what constitutes a computer crime. One reason is the rapidly changing state of computer technology. For example, in 1979, the U.S. Department of Justice publication [6] partitioned computer crime into three categories: 1) Computer abuse, "the broad range of international acts involving a computer where one or more perpetrators made or could have made gain and one or more victims suffered or could have suffered a loss;" 2) Computer crime, "illegal computer abuse [that] implies direct involvement of computers in committing a crime;" and 3) Computer-related crime, "any illegal act for which a knowledge of computer technology is essential for successful prosecution." These definitions have become blurred by the vast proliferation of computers and computer related products over the last decade. For example, does altering an inventory bar code at a store constitute computer abuse? Should a person caught in such an act be prosecuted under both theft and computer abuse laws? Clearly, advances in computer technology should be mirrored by parallel changes in computer law.

Another attempt to describe the essential features of computer crime has been made by Wolk and Luddy [1]. They claim that the majority of crimes committed against or with the use of a computer can be classified as follows:

> Sabotage: "Involves an attack against the entire [computer] system or against its subcomponents, and may be the product of foreign power involvement or penetration by a competitor..."
> Theft of services: "Using a computer at someone else's expense."
> Property crimes involving the "theft of property by and through the use of computers." [7]

A good definition of computer crime should capture all acts which are criminal and involve computers and only those acts. Assessing the completeness of a definition seems problematic, but is tractable using technical computer security concepts.   For example, consider the following matrix:

	Confidentiality	Integrity	Availabilityh
Sabotage		X	X
Theft of Services			X
Property Crimes	X		X

This shows that Wolk and Luddy's categorization is strong with respect to availability and weaker in the areas of confidentiality and integrity. Indeed, upon closer examination it becomes apparent that there are ways to violate confidentiality and integrity which do not constitute sabotage, theft of services, or property crimes. For example, a Trojan horse could append code to a word processor which sends copies of a user's confidential text as messages to the perpetrator's electronic mailbox. This isn't sabotage because no AIS functionality was destroyed or even altered; theft of services does not apply if the perpetrator is paying for his electronic mail account; and unless the confidential text was copyrighted, it is not a property crime. This analysis is significant because it demonstrates that examining a legal concept from a technical perspective can yield insights into its strengths and weaknesses and even suggest avenues for improvement.

Conclusion

The development of effective computer security law and public policy cannot be accomplished without cooperation between the technical and legal communities. The inherently abstruse nature of computer technology and the importance of the social issues it generates demand the combined talents of both. At stake is not only a fair and just interpretation of the law as it pertains to computers, but more basic issues involving the protection of civil rights. Technological developments have challenged these rights in the past and have been met with laws and public policies which have regulated their use. For example, the invention of the telegraph and telephone gave rise to privacy laws pertaining to wire communications. We need to meet advances in automated information technology with legislation that preserves civil liberties and establishes legal boundaries for protecting confidentiality, integrity, and assured service. Legal and computer professionals have a vital role in meeting this challenge together.

REFERENCES

[1] Stuart R. Wolk and William J. Luddy Jr., "Legal Aspects of Computer Use," Prentice Hall, 1986, pg. 129.

[2] National Computer Security Center, "Glossary of Computer Security Terms," 21 October 1988.

[3] Thomas R. Mylott III, "Computer Law for the Computer Professional," Prentice Hall, 1984, pg. 131.h [4] Gasser, Morrie, "Building a Secure Computer System," Van Nostrand, 1988.

[5] Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985.

[6] United States Department of Justice, "Computer Crime, Criminal Justice Resource Manual," 1979.

[7] Wolk and Luddy, pg. 117.