A Review of Internet Crime

Ernst L. Leiss [1]
[S1]
Department of Computer Science, University of Houston
Houston Texas 77204-3010, USA
coscel@cs.uh.edu

Abstract. We distinguish crimes that merely use the Internet as facilitator from those that require it. This starts a discussion of the fundamental differences between cyber and ordinary crime. Important for the existence of a crime is the requirement for a law that creates that crime. Since laws tend to be local while the Internet is global, a significant tension arises between the various goals and objectives of differing jurisdictions on the one hand and the global reach of the Internet on the other. We illustrate with two examples, the distribution of pornography and cryptographic methods. A third type, child pornography, is sui generis and has the potential of creating significant problems for the computing community. We then discuss protections against cyber crime. While legal means purport to provide protection, it is only technical means that afford a measure of protection against some of these crimes.

Keywords: Cyber crime, distributed denial of service, spy ware, spam, spoofing, phishing, intellectual property.

1 Introduction

The object of this paper is Internet crime. In view of our discussion below, we aim to widen the semantics of the word ‘crime’ meaningfully. Therefore, in the following we will use the word ‘crime’ to circumscribe activities that are either considered criminal in a significant number of countries where the Internet is used, or are generally considered to be extremely undesirable and detrimental to society at large. This is a significantly more general definition of crime than often used; in particular, it does not coincide with the common legal definition and as such does not have direct applicability, especially as it relates to finding guilt and meting out punishment. We discuss later the controversies that this may engender. Here we observe that the term ‘Internet crime’ does not necessarily imply universality. Indeed, an important aspect of the legal environment involving the Internet is precisely the problem that different countries wish to apply their local standards to a global commodity.

With this caveat in mind, we start by differentiating between two different types of crime, namely ordinary crimes that are facilitated by the Internet, and crimes that

[1] Support of this research under NSF grants DUE 0313880, SCI 0453498, and OISE 0519316 is acknowledged.

essentially depend on the existence of the Internet; in other words, the latter type of crimes would virtually disappear, were the Internet to disappear. We believe that this distinction is useful for an examination of relevant issues, even though there are activities that can (and will) be listed under both rubrics.

2. Common Crimes Facilitated by the Internet

2.1 Common crimes with economic purposes or motivation: These crimes are probably less interesting from the point of view of informatics, in that their criminality is fairly clear-cut; however, they are probably the most lucrative ones. They are generally recognized crimes, in that virtually all countries have laws against them. (While this might not have been true some years ago for electronic fund transfers and intellectual property [IP], even lesser developed countries have today recognized in their legal systems the power of cyber crooks to do harm.) The most important ones are:

Theft of funds through electronic means
Espionage
Theft of intellectual property (IP)

Essentially, these are ordinary crimes where the computer system (computers, networks, etc.) is a tool. This tool may make it easier, in some case dramatically so, to commit the crime, but the crime could just as well be committed using old-fashioned means (that is, using weapons or other threats, blackmail, or break-ins).

Interesting and frequently quite important is the fact that the use of a computer environment often makes detection of the crime more difficult: it may take a relatively long time to detect that a crime has been committed. While automatic audit facilities are common, audit trails require frequently extensive involvement by humans, which can increase the reaction time substantially.

Also, the immediacy of such a crime is frequently obscured: If I obtain $10,000 by robbing a bank, for example by threatening the bank teller with a gun, law enforcement tends to react very rapidly – this is something the police knows and understands. If I obtain $10,000 by subverting a bank's electronic fund transfer (EFT) system, it is much more difficult to obtain appropriate support and reaction from law enforcement. Furthermore, there is the problem of thresholds: While any bank would insist on prosecuting the perpetrator of a hold-up resulting in $10,000, it may be much more difficult to get a bank and a prosecutor to go after a cyber crook who got away with $10,000 (unless the same trick could be used repeatedly and possibly for much larger sums!). It is of course true that the bank robber is in actual possession of the bank notes, while the successful attacker of the EFT system still has to find a way of getting his hands on the money, but this has ironically been made easier by technology – since the stolen funds can be transferred using EFT to less scrupulous banks in countries with fewer safeguards!

Espionage (I am interested only in industrial espionage; military or diplomatic secrets of any significance are becoming fewer and fewer and certainly do not hold any great economic promise) is an old activity that has however been streamlined through the use of computer networks to transmit, and computer systems to collect, analyze, and store, such information. Again, it is the computing environment that

facilitates the activity, but the activity itself had been well established long before the advent of computers. Nevertheless, it should be recognized that viruses and worms can be programmed to search for files containing certain key words and to post these files in a location that the crook can access. Furthermore, the compactness of memory sticks and CD-ROMs is a significant aid in smuggling extensive documentation out of relatively secure areas. (While the use of the Internet might be viewed as helping in such smuggling activities as well, generally the opposite is true: It is relatively easy to define and enforce policies that prevent this. Whether these steps are in fact taken and the policies enforced is a different question, one that has nothing to do with computer systems and everything with human nature!)

Theft of IP is a somewhat more recent topic, although for the most part, it is also well-established and quite wide-spread. This may relate to software (large amounts of economic losses are claimed by software vendors due to piracy) or video and audio (illicit copies of numerous first-run movies appear distressingly fast on a parallel market; huge volumes of songs are exchanged, often in violation of copyright laws, by individuals using peer-to-peer [P2P] file sharing systems). This theft can be a commercial activity with an explicit profit motive (as in the case of most illicit software and DVDs of newly released movies) or the acts of individuals whose interest is simply in avoiding having to pay a few dollars for a CD containing the music. In the latter case, it is primarily the large volume of infractions (and the concomitant decline in sales of CDs!) that is responsible for the recognition of the crime and the increased efforts by the holders of the copyright to prosecute it.

2.2 Vandalism: Vandalism is old and well established; however, using computers it can become much more destructive and much more difficult to prevent. We mention:

Viruses and worms
Denial of service

Viruses have first been demonstrated in 1983; however, while they initially spread in slow and cumbersome ways (bulletin boards, exchange of files stored on diskettes), their distribution has dramatically accelerated through the use of the Internet. Today, it is extremely ill-advised not to use virus (and worm) detection products routinely, repeatedly, and rigorously. While many viruses and worms have the ability to corrupt extensively their victims' computer systems, most of them only destroy data – thus, they are vandals. Of course, a secondary aspect of these attackers is that the victims are unable to use their systems for prolonged periods of time, effectively resulting in denial of service.

Denial of service (DoS) can be the result of an infection by a virus or worm; however, more frequently DoS refers to the malicious overwhelming of a website by means of spurious requests, to the extent that the website collapses. Today, most DoS attacks are distributed: The attacker manages in some way to install copies of the attacking program on many, perhaps tens or hundreds of thousands of computers, which, at a point in time controlled by the attacker, launch in a coordinated fashion their attacks (spurious requests for service) on the target. Generally, it is difficult to distinguish a DDoS from a legitimate heavy load of the system, at least until it is too late.

3 Internet Crimes

Here we are interested in crimes specifically related and intimately connected with the Internet. We mention:

Distributed denial of service
Spy ware
Spam
Spoofing, phishing
Violation of copyrights of IP
Distribution of undesirable material of information

While distributed denial of service (DDoS) is conceivable without the Internet, it is today only the Internet that provides the environment where such attacks can flourish. The typical mode is the installation of programs on many different (and usually unsuspecting) computer systems via the Internet, often as the payload of some virus or worm; these widely dispersed programs then carry out the actual attack. Numerous sites have been the target of DDoS attacks of varying degrees of maliciousness.

Spy ware is software that monitors a computer user's activities and has the ability of either reporting actively, or be queried remotely about, the recorded activities. This includes highly confidential information, such as passwords, credit card numbers, and PIN codes, all of which may typically be typed in by the user at some point, making them subject to interception by the spy ware program. In fact, spy ware programs can record all sites that a victim visited. They are clearly a major tool for privacy violations. The installation of spy ware tends to be similar to that of the programs involved in a DDoS attack. ActiveX and software of a similarly powerful nature are frequently implicated here. Unfortunately, many users tend to cavalier about permitting such processes to execute tasks on their computers about whose trustworthiness they know very little.

Spam is essentially any mail that the recipient does not like to receive. This definition clearly indicates the problem with it: there is no universal definition. What one person considers spam may be considered very useful information by someone else. Thus, the universal, automatic elimination of spam is virtually impossible. While there exist challenge-response systems that help cut down on the prevalence, they are somewhat cumbersome to use and therefore frequently avoided. (The idea is to force the sender to validate each message by proving that the sender is a human, and not a program that spews out millions of messages each hour. Such proofs typically involve posing problems that can easily solved by a human, but are very hard for a computer. Such problems usually involve character or pattern recognition. This is actually an interesting application of artificial intelligence: designing problems that are easy for humans but hard for computers to solve.) Spam is deeply related to the overall business model of the Internet: It does not cost anything to send a file. Therefore, spammers can send literally millions of messages, at little to no cost to them.

Spoofing and phishing are aspects of social engineering whereby the attacker attempts to persuade the victim to part with important personal information, such as numbers of financial accounts, PINs, credit or debit card numbers, and other information, the knowledge of which enables the attacker to steal the victim's identity. Usually, the request for this information is contained in a spam message. Often, the user is asked to go to a web site that looks just like the legitimate web site

of a bank or other institution, but is in fact a fake site created by the attacker for the sole purpose of collecting confidential information. With this information, the successful attacker can impersonate the victim and wreck havoc with the victim's financial well-being. This is generally referred to as identity theft and is a growing problem in the US. For example, the attacker can use the personal information of the victim to apply for credit cards (in the victim's name!) and use up the credit lines that come with them. Again, it is the business model of the Internet that enables successful phishing and spoofing, since an attacker can send out millions of spam messages pretending to be a legitimate bank or PayPal system requesting personal information, and it is sufficient that a tiny fraction of the recipients (perhaps one or two in a million!) falls for the scam to be financially rewarding to the crook. In general, one should never respond to any request for financial information received via the Internet. It should be clear that by its very nature, there are no technical means to prevent this activity, since it is the user who volunteers the information. In other words, there are no technical solutions to prevent a user's stupidity!

Violation of the copyrights of IP was mentioned earlier; however, the advent of P2P file exchange systems, such as BitTorrent, is intimately related to the Internet environment. Today, these systems tend to be fully distributed, in contrast to earlier file-sharing methods that were centralized and could therefore be easily targeted for prosecution and subsequent shut-down by law enforcement. While some people make arguments that copyright should be redefined since it does not meet the needs of a digital society (only the most extreme advocate the outright abolition of copyright), at present all industrial and most developing countries recognize copyright provisions. Many in fact are signatories of the World Intellectual Property Organization (WIPO) which is the counterpart of the better-known World Trade Organization (WTO). WIPO has as one of its main objectives the harmonization of IP issues (mainly of a legal nature), primarily copyright and patent provisions across all of its member states.

Finally, it should be clear that the Internet is monumentally implicated in the distribution of illicit or undesirable material or information. This is an area where there is a significant amount of disagreement, among different people of the same society, and even more so among different societies and nations. Indeed, various countries strenuously insist on the right of restricting the access of its citizens to certain information. For example, the People's Republic of China (PRC) restricts not just access to information, but has also forced companies such as Google to restrict their search engines to government acceptable sites. Below we will have a closer look at two very controversial topics, at two ends of the technology spectrum, namely using the Internet for the distribution of pornography and for the distribution of cryptographic techniques.

Before we address these topics, we must explore in some detail the fundamental underpinnings of the definition of crime and contrast it with the worldview underlying the Internet. This will allow us to understand the tension between the tendency of jurisdictional entities to ban certain activities and the tendency of the Internet to be all-permissive, functioning merely as a conduit without taking any position as to the legality of any action involving the Internet.

4 What Is a Crime?

Fundamentally, an action can be a crime only if there exists a law that makes it explicitly a crime. Absent a law criminalizing an activity, the activity cannot be a crime. (It may be unethical, immoral, or reprehensible, but without a law, there cannot be a crime and consequently no judicial punishment.) A very important aspect of this is that it is exclusively tied to a state. This in particular implies that crimes tend to be local – restricted to one nation where that nation's law makes the activity a crime. In extreme cases, we have situations where someone who commits an act that country A considers a crime and who escapes to country B where that act is not considered a crime will not be extradited by country B upon request of country A, because B argues that the perpetrator should not be punished since in B the act is not illegal.[2]

Now consider the Internet: It spans every inhabited time zone, is not tied to a specific country and its legislation (even though there are frequently complaints that the US is dominant in the administration of the Internet – but would we rather have the PRC run it?), and therefore spans many countries with vastly different concepts of what is illegal or criminal. If one wanted to define criminal action involving the distribution of some material, which country's laws should apply: The country **from** which the material was sent? The country **to** which the material was sent? Or even a country **through** which the sequence of bits embodying the material passed?

Generally and for historical reasons, the Internet community has not been interested in prohibiting anything. Effectively, an 'anything goes' attitude has prevailed from its inception. This permissiveness has led to accusations that the Internet aids and abets in all kinds of crimes, from child pornography to treason. Internet advocates respond that its function is nothing other than that of a highway – just because criminals use the highway does not mean it should be shut down or its use severely restricted.

It can easily be inferred from these comments that this tension is unlikely to disappear or even abate in the foreseeable future. In order to illustrate some of the issues involved, we consider two case studies, namely the involvement of the Internet in the distribution of pornography and of cryptographic methods. For both instances, we explain the contradictory objectives without offering any solution for reconciling them.

5 Two Case Studies

Let us look at two specific types of material that countries are wont to regulate or ban, namely pornography and cryptographic techniques. In both cases, I will focus on the US because I know the situation there best and because it is to some extent a microcosm of much that is to be considered.

---

[2] Perhaps the greatest divergence is in assisted suicide – some countries prosecute anyone assisting in it for homicide which might incur length prison sentences, other countries consider it entirely lawful to help an individual to commit suicide.

Pornography is a very controversial topic. In many countries the regulation of pornography clashes with the principle of freedom of speech. This is certainly the case for the US. To date, there does not exist a universal definition of pornography; instead, the United States Supreme Court has declared that 'community standards' are to be used in deciding whether specific material should be considered pornographic. Thus, material that would be considered clearly non-pornographic in the Tenderloin district of San Francisco (an area with extremely lax community standards) would most likely be held pornographic in many rural areas in Kansas. This approach was somewhat workable (although there have always been vocal dissenters, on both sides of the discussion) as long as the distribution of potentially pornographic material was through the mail, as printed matter (books, magazines). However, distributing material over the Internet changes the legal paradigm dramatically. What if the sender resides in the Tenderloin district, but the recipient lives in rural Kansas? While it may be clear that the recipient of (according to local community standards, in Kansas) pornographic material commits a crime, what about the sender? If this were so, senders would have to know exactly the legal situation in each place to which they ship! What about a situation where a transmission from one place of lax standards to another place of lax standards passes through a locality with restrictive standards? (The nature of the Internet is such that no guarantees can be given whether or not a certain site participates in any given transmission.) In this latter case, may both sender and receiver be prosecuted under the restrictive community standards of the intermediary? While this last case has not been tested in the courts, the second case (with the sender in California and the recipient in Kansas) has – with the sender having been convicted for the distribution of pornographic material under the restrictive community standards of the recipient!

Cryptographic techniques are frequently considered important state secrets by various governments. Numerous countries attempt to regulate their distribution. Within the US, these attempts have historically been defeated by invoking the constitutionally guaranteed freedom of speech. However, as the US Constitution applies only within the US, the US Government has prohibited the export of (strong) cryptographic techniques. (Strictly speaking, this statement is false: The US requires that one obtain an export license if one wants to take a strong cryptographic technique to a foreign country. The only problem is that this license is never granted…) Strong is typically defined with respect to the length of the encryption keys involved in an encryption method. Exempting weaker methods (that is methods with shorter keys) is merely a recognition that some type of encryption is desirable – just not any that the NSA cannot break!

There are numerous problems with this approach, not the least of which the fact that the only provably unbreakable code, namely one-time random pads, has been known for over 80 years, in most countries with any interest in cryptography. However, here we look at the role of the Internet. If I wanted to send my friend in the same city a copy of some cryptographic algorithm using the Internet, I might be actually violating the law regulating the export of such techniques, because I have no guarantee that the transmission to that person next door might not pass through a foreign country. Certainly the Internet does not provide any such assurances. Moreover, if I were to bring, on my laptop computer, a strong cryptographic algorithm back from a trip abroad, I am entitled to do so: import is not restricted.

However, if I subsequently take the same laptop with that same algorithm out of the country, for example back to the country from which I imported the cryptographic algorithm, I am now technically in violation of the law!

It should be clear that in both scenarios, the involvement of the Internet in the distribution of digital material creates new and unforeseen problems, mainly of a legal nature. To date, these issues are largely unresolved, even within the US, and therefore much more so when they involve more than one jurisdiction.[3]

6 Child Pornography

Child pornography is quite universally reviled; most countries criminalize not just the production, but also the distribution and possession of such material. Child pornography is not dependent on the Internet, although its availability has greatly increased the opportunities for the distribution of such material, typically images and videos. Nevertheless, child pornography creates particular problems for the computing community, as we indicate below.

Historically, the impetus for the criminalization of child pornography has been the protection of minors involved, virtually by definition involuntarily, in the production of images and videos/movies. In recent years, this has been extended to include cartoons and other material whose production clearly did not involve minors.

The situation becomes much more complicated because of the existence of software that allows producing images of people of certain ages, based on photographs of these people at a different age. Anyone who has seen posters aiding in the search of children kidnapped years ago is familiar with this type of aging software. Essentially, certain principles of human development are applied to a given person's image in order to obtain an image of how that person likely looks after a specified number of years. The computing community's problem stems from the fact that this aging software can be run backwards, that is, instead of making the person older, we can equally make a person younger.

Applying such aging software backwards to an image (or video) of certain sexual activities that would be entirely lawful to produce, distribute, and possess could result in material that clearly falls under the rubric of child pornography. In fact, it would even be conceivable that anyone who wishes to possess child pornography stores such material only in its aged ("older") form, thus rendering the images lawful, and only views the material applying the reverse aging software. In this way, no illegal images are ever stored and the viewing process, assuming the backward-aging software can be run in real time, would guarantee that the illegal material exists only in its most ephemeral form, as a display with no permanence whatsoever.

It should be clear that software is a crucial element is this scenario; it is essentially the software that creates the illegal images, using as input lawful and lawfully

[3] A note for legal scholars: Criminal law in the US is predominantly a state matter; few criminal laws are federal in the US. Thus, there are at least 52 different jurisdictions in the US (50 states plus the District of Columbia, as well as the Federal Government). In fact, there are many more, since municipalities for example also have jurisdictional powers, albeit usually at a lower level.

obtained images. At the same time, one would not expect reasonable people to argue that such software should be made illegal. Furthermore, if the basis for the criminalization of child pornography (as opposed to ordinary pornography) is the protection of minors, it is a bit of a stretch to see why the ability of taking the image of a twenty-something performer and dialing back that actor's age by a certain number of years should provide illegal content. At any rate, different country may have different approaches to this problem. What should be clear is that the introduction of computer software that allows one to change the perceived age of a performer has introduced significant legal complications.

7 Protections Against Internet Crime

In view of the apparent ubiquity of cyber crime, the need for protection appears paramount. There are legal protections and there are technical protections. It is traditionally accepted to talk about legal protections; however, I maintain that 'legal protections' really do not protect: If laws against murder protected people against being murdered, nobody would be murdered. We all know that this is of course false – everyday people are murdered, in spite of the law's supposed protection. What the law does instead is provide for punishment if the law is breached – something that is very different from a true protection.

This clarification is important since we do have certain technical approaches which indeed do protect: To see this, observe that it is impossible to understand a file that is encrypted (with a strong encryption method), unless one has the appropriate decryption key. Thus, if one wants to protect the file from being read by unauthorized persons, this protection can be provided by purely technical means.

There are several general schemes that find extensive use as mechanisms for protecting against the cyber crime we have discussed. The main ones are:

Encryption
Authentication techniques, including certificates
Digital watermarks

Encryption can be used, frequently in conjunction with various protocols, to achieve security and integrity of digital media. Security refers to granting (read) access only to those who are authorized to access. Integrity refers to the question whether the digital media object was altered (from a technical point of view, the term refers to write access). Thus, security is concerned with restricting access, while integrity is concerned with ensuring that the information is original, has not be modified unbeknownst to the user (or even to the owner). In addition, most Digital Rights Management (DRM) systems employ encryption in some form.

Encryption has been documented going back to Julius Caesar's writings. For a long time it was considered under military control. However, in the last three decades, most important advances in cryptography have been made by civilians. Foremost among these is public-key cryptography which is widely used in today's security certificates that are employed for secure communications. While public-key cryptography has several practical advantages over classical or symmetric cryptography (for example, in contrast to classical methods there is no need for prior

key exchange, allowing users who have never been in contact to exchange messages securely), symmetric encryption schemes will continue to be widely used because of complexity considerations (their time complexity typically is linear, making them very suitable for the real-time transmission of large files).

Authentication is an important aspect of preventing cyber crime: if a perpetrator had to identify himself before carrying out his actions, it would reduce cyber crime very significantly. Historically, authentication within the digital realm has been done using passwords. Passwords have the advantages of compactness (they are small, on the order of tens of bytes) and that they can be changed easily. They have the disadvantage that they are not tied uniquely to a specific user: several users may use the same password (without knowing it). Another way of authenticating a user is via a physical device, a smart card or a dongle. Such devices tend to be cumbersome and can be lost or stolen. A third approach employs biometric measurements, such as fingerprints, hand geometry, iris or retina scans, or voice or face recognition schemes. Their primary advantage is the very close connection between the measurements and the person – it is essentially undesolvable (e. g., one cannot get new finger prints, if the data pertaining to the old ones were lost). This is of course also a disadvantage, in addition to some technical aspects which include the large size of the data sets, up to tens of kilo bytes (or up to three orders of magnitude larger than for passwords) and the need for a similarity function to determine matches. This is an important issue in authentication based on biometric measurements; much in contrast to passwords, where it is an exact match that is required, a similarity function is needed since two physical measurements will never be identical. However, if the similarity requirements are too strict, legitimate users will be denied access (false-negative); if the requirements are too relaxed, unauthorized users will be erroneously granted access (false-positive). It is very difficult to obtain a practical method that has no false-positives and a very low percentage of false-negatives.

Digital watermarks have attracted attention in the past few years, primarily because they permit the safeguarding of the integrity of a digital object, usually without affecting its use in any perceptible way. They can be used to mark individual copies of the same object uniquely, thereby permitting the tracing of these objects, even when they pass through various hands. Moreover, digital watermarks tend to survive various common manipulations and most importantly are copied whenever a watermarked object itself is copied. Thus, it is possible to determine from which legitimate watermarked copy an illegal copy was made.

In addition to these specific and targeted techniques, the design, production, and distribution of safe software is highly desirable if one wants to reduce cyber crime. Too much software in use today is riddled with vulnerabilities that are built into the software, either because of an ill-conceived desire for efficiency or because of sloppiness. Even software produced today contains vulnerabilities that have been identified for a long time. A primary example is given by buffer overflows. A buffer overflow occurs when a data structure designed for a certain amount of data is filled with more than that amount of data. It is of course trivial to write code that detects an attempt to cram more data into the structure than it can hold, but such a test requires a certain amount of time to carry out (at run time). Since it must be carried out every time data are entered into the structure, incompetent programmers often decide to save this execution time by foregoing the test whether the buffer is overwhelmed by

too much data. Many of today's viruses and worms exploit (unchecked) buffer overflows. Eliminating this obvious and well-documented vulnerability would eliminate much of today's viruses and worms. The fact that these attackers are still alive and well and wrecking havoc on our systems is testimony to the prevalence of unchecked buffers in our software.

Vulnerabilities in general are most likely unavoidable; one must keep firmly in mind that today's software is far more complex than any other human creation. In particular, software is unique in that a small change in one module can have totally unexpected consequences in a very different module. Thus, it will probably be always necessary to install periodically patches that remedy problems and vulnerabilities which were discovered during the use of the software. We can only hope that employing sound design principles will reduce the frequency of these patches.

8 Conclusion

Cyber crime has many facets; this makes it vastly more challenging to combat than ordinary crime. In addition, while one might take solace in the fact that there are fewer such criminals, they are probably much smarter than the average criminal. This creates problems for law enforcement – the typical thief has a profile that differs dramatically from the profile of someone who subverts an EFT system to steal money, even though the outcome may be the same: theft occurred.

For some aspects of cyber crime, there exist technical solutions or protections; the fundamental problem is to get people to employ them. An additional complication is the question where and by whom these solutions and protections can be applied. Clearly, if I am a user of an operating system, I have very little influence on the question whether it handles buffer overflows correctly. In this case, I can only hope that by installing every patch diligently and quickly, I can protect myself against threats that have already affected some users. (One should recognize that the typical mode of operating in the patch business is reactive: only once a vulnerability is detected by some users, patches addressing the uncovered problem are produced and distributed. Moreover, there have be incidents where a company reacted by producing a patch only after a vulnerability was exploited by crooks, even though the company had been informed of that vulnerability long before it was exploited.) On the other hand, if I distribute digital media objects over the Internet, I have available several methods that allow me to achieve objectives of security or integrity, for example, encryption or digital watermarking schemes.

Users concerned about cyber crime have several technical means to protect themselves and their digital assets. It is important that all users be aware that cyber crime is quite ubiquitous and that the inconvenience of employing these technical protections is certainly dwarfed by the difficulties the user encounters once he becomes a victim of cyber crime.

9 Bibliographical Notes

[2] is an overview of security and integrity issues related to activities involving the Internet, including e-commerce, the use of certificates in secure communications, various types of attacks, and public policy topics. [8] is an all-encompassing compendium of encryption methods, including one-time random pads, the only provably unbreakable encryption scheme; see also [3]. [1] introduced public-key cryptography in a seminal paper, a hugely influential notion without which much of today's secure Internet communication would not function. Viruses and worms are discussed in [4]. Digital watermarks and their use are described in [5]; more extensive references can be found there. The advantages and disadvantages of passwords and biometric measurements are discussed in [6, 7], together with other aspects of authentication.

References

1. W. Diffie and M.E. Hellman: New directions in cryptography, *IEEE Transactions on Information Theory* **22** (1976), 644-654
2. S. Garfinkel: *Web Security, Privacy, and Commerce*, Second Edition, O'Reilly and Associates, Sebastopol (2002).
3. E. L. Leiss: *Principles of Data Security*, Plenum Publishing Corporation, New York, NY (1982).
4. E. L. Leiss: *Software Under Siege: Viruses and Worms*, Elsevier, Oxford, 1990.
5. E. L. Leiss: Time-Variant Watermarks for Digital Video: An MPEG-Based Approach, in *Digital Watermarking for Digital Media*, J. Seitz (ed.), Idea Group Publishing, Hershey, PA (2005).
6. E. L. Leiss: Safeguarding the Transmission of Biometric Measurements Used for Authenticating Individuals, Proc. IFIP World Computing Congress, NetCon, Santiago, Chile, August 20-25 (2006).
7. E. L. Leiss: Requirements for the Safe Transmission of Biometric Measurements for Authenticating Individuals, CLEI 2008 – Conferencia Latinoamérica de Informática, Sept. 1-5, Santa Fe, Argentina (2008).
8. B. Schneier: *Applied Cryptography*, Second Edition, John Wiley and Sons, New York (1996).