Other Efforts to Secure Data in Computer Networks and Beyond

20

20.1 Introduction

The rapid advances in computer technology, the plummeting prices of information processing and indexing devices, and the development of sprawling global networks have all made the generation, collection, processing, indexing, and storage of information easy. Massive information is created, processed, and moved around on a daily basis. The value of information has skyrocketed, and information has all of a sudden become a valuable asset for individuals, businesses, and nations. The security of nations has come to depend on computer networks that very few can defend effectively. Our own individual privacy and security have come to depend on the whims of the kid next door.

Protection of information, on which we have come to depend so much, has been a major challenge since the birth of the Internet. The widespread adoption of computer technology for business, organization, and government operations has made the problem of protecting critical personal, business, and national assets more urgent. When these assets are attacked, damaged, or threatened, our own individual, business, and more importantly national security is at stake.

The problem of protecting these assets is becoming a personal, business, and national priority that must involve everyone. Efforts and ways must be sought to this end. But getting this massive public involvement will require massive public efforts on several fronts including legislation, regulation, education, and activism. In this chapter, we examine these efforts.

20.2 Legislation

As the Internet Web grows, Internet activities increase, e-commerce booms, and globalization spreads wider, citizens of every nation infuriated by what they see as the "bad" Internet are putting enormous and growing pressures on their national legislatures and other lawmaking bodies to enact laws that would curb cyberspace

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_20

activities in ways that they feel best serve their interests. The citizens' cause has been joined by special interest groups representing a variety of causes such as environmental protection, free speech, intellectual property rights, privacy, censorship, and security.

Already this has started happening in countries such as the United States, United Kingdom, Germany, France, China, and Singapore, and the list grows every passing day. In all these countries, laws, some good, many repressive, are being enacted to put limits on activities in cyberspace. The recent upsurge of illegal cyberspace activities such as the much publicized distributed denial of service and the headline-making e-mail attacks has fueled calls from around the world for legislative actions to be taken to stop such activities. Yet it is not clear and probably unlikely that such actions will at best stop and in the least arrest the escalating rate of illegal activities in cyberspace. Given the number of cyberspace legislations we presently have in place and the seemingly escalating illegal cyberspace incidents, it looks like the patchwork of legislation will not in any meaningful way put a stop to these malicious activities in the near future. If anything, such activities are likely to continue unabated unless and until long-term plans are in place. Such efforts and plans should include first and foremost ethical education.

Besides purely legislative processes which are more public, there are also private initiatives that work either in conjunction with public judicial systems and law enforcement agencies or work through workplace forces. Examples abound of large companies, especially high-technology companies such as software, telecommunications, and Internet providers coming together to lobby their national legislatures to enact laws to protect their interests. Such companies are also forming consortiums of some form or partnerships to create and implement private control techniques.

20.3 Regulation

As the debate between the freedom of speech advocates and children's rights crusaders heats up, governments around the world are being forced to revisit, amend, and legislate new policies, charters, statutes, and acts. As we will see in detail in the next section, this has been one of the most popular and, to politicians, the most visible means of dealing with the "runaway" cyberspace. Legislative efforts are being backed by judicial and law enforcement machinery. In almost every industrialized and many developing countries, large numbers of new regulations are being added to the books. Many outdated laws and acts are being revisited, retooled, and brought back in service.

20.4 Self-Regulation

There are several reasons why self-regulation as a technique of cyberspace policing is appealing to a good cross section of people around the globe. One reason, supported mostly by the free speech advocates, is to send a clear signal to governments around the world that the cyberspace and its users are willing to self-regulate, rather than have the heavy hand of government decide what is or is not acceptable to them.

Second, there is realization that although legislation and enforcement can go a long way in helping to curb cyber crimes, they are not going to perform the magic bullet that will eventually eradicate cyber crimes. It should be taken as one of a combination of measures that must be carried out together. Probably, one of the most effective prevention techniques is to give users enough autonomy to self-regulate themselves, each taking on the responsibility to the degree and level of control and regulation that best suits his or her needs and environment. This self-regulation cyberspace can be done through two approaches: hardware and software.

20.4.1 Hardware-Based Self-Regulation

There is a wide array of hardware tools to monitor and police cyberspace to a degree suited for each individual user of cyberspace. Among the tools are those individually set to control access, authorization, and authentication. Such hardware tools fall mainly in six areas, namely:

- *Prevention*: Prevention is intended to restrict access to information on the system resources such as disks on network hosts and network servers using technologies that permit only authorized people to the designated areas. Such technologies include, for example, firewalls.
- *Protection*: Protection is meant to routinely identify, evaluate, and update system security requirements to make them suitable, comprehensive, and effective.
- *Detection*: This involves deploying an early warning monitoring system for early discovery of security breaches both planned and in progress. This category includes all intrusion detection systems (IDS).
- *Limitation*: This is intended to cut the losses suffered in cases of failed security.
- *Reaction*: To analyze all possible security lapses and plan relevant remedial efforts for a better security system based on observed failures.
- *Recovery*: To recover what has been lost as quickly and efficiently as possible and update contingent recovery plans.

20.4.2 Software-Based Self-Regulation

Unlike hardware solutions which are few and very specialized, software solutions are many and varied in their approaches to cyberspace monitoring and control. They are also far less threatening and therefore more user-friendly because they are closer to the user. This means that they can either be installed by the user on the user's computer or by a network system administrator on a network server. If installed by the user, the user can set the parameters for the level of control needed. At a network level, whether using a firewall or specific software package, controls are set based on general user consensus. Software controls fall into three categories [1]:

- *Rating programs*: Rating programs rate cyberspace content based on a selected set of criteria. Among such criteria are violence, language, and sex content. Software rating labels enable cyberspace content providers to place voluntary labels on their products according to a set of criteria. However, these labels are not uniform for the whole industry; they depend on a rating company. There are many rating companies, including CyberPatrol, CYBERsitter, Net Nanny, and SurfWatch, all claiming to provide a simple yet effective rating system for Web sites to protect children and free speech of everyone who publishes in cyberspace. These labels are then used by the filtering program on the user's computer or server.
- *Filtering programs*: Filtering software blocks documents and Web sites that contain materials designated on a filter list, usually bad words and URLs. They always examine each Web document header looking for matching labels to those on the "bad" list. Filters are either client based, in which a filter is installed on a user's computer, or server based, in which they are centrally located and maintained. Server-based filters offer better security because they are not easy to tamper with. Even though filtering software has become very popular, it still has serious problems and drawbacks such as inaccuracies in labeling, restriction on unrated material, and just deliberate exclusion of certain Web sites by an individual or individuals.
- *Blocking*: As we discussed in Chap. 14, blocking software works by denying access to all except those on a "good" list. Blocking software works best only if all Web materials are rated. But as we all know, with hundreds of thousands of Web sites submitted every day, it is impossible to rate all materials on the Internet, at least at the moment.

20.5 Education

Perhaps one of the most viable tools to prevent and curb illegal cyberspace activities is through mass education. Mass education involves teaching as many people as possible the values of security, responsible use of computer technology, how to handle security incidents, how to recover from security incidents, how to

deal with the evidence if legal actions are to be followed, and how to report security incidents. Although mass education is good, it has its problems including the length of time it takes to bear fruits. There are many people still not convinced that education alone can do the job. To these people, there is no time; if action is to be taken, then the time to do so is now. However, we are still convinced that the teaching of ethical use of computer technology, as long as it takes, always results in better security measures than what else we have discussed so far. For without ethics and moral values, whatever trap we make, one of us will eventually make a better trap. Without the teaching of morality and ethics, especially to the young, there is likely to be no break in the problems of computer and network security. Along these lines, therefore, education should be approached on two fronts: focused and mass education.

20.5.1 Focused Education

Focused education targets groups of the population, for example, children in schools, professionals, and certain religious and interest groups. For this purpose, focused education can be subdivided into formal education and occasional education.

Private companies are also conducting focused education. For example, there are a number of private companies conducting certification courses in security. These companies include Computer Science Institute (CSI), Cisco, Microsoft, SANS Institute, and others.

20.5.1.1 Formal Education

Formal education targets the whole length of the education spectrum from kindergarten through college. The focus and contact, however, should differ depending on the selected level. For example, in elementary education, while it is appropriate to educate children about the dangers of information misuse and computer ethics in general, the content and the delivery of that content are measured for that level. In high schools where there is more maturity and more exploratory minds, the content and the delivery system get more focused and more forceful. This approach changes in colleges because here the students are more focused on their majors, and the intended education should reflect this.

20.5.1.2 Occasional Education

Teaching morality, ethics, computer security, and responsible use of information and information technology should be lifelong processes just how teaching responsible use of a gun should be to a soldier. This responsibility should be and is usually passed on to the professions.

There are a variety of ways professions enforce this education to their members. For many traditional professions, this is done through introduction and enforcement of professional codes, guidelines, and cannons. Other professions supplement their codes with a requirement of in-service training sessions and refresher courses.

Quite a number of professions require licensing as a means of ensuring continuing education of its members. It is through these approaches of education that information security awareness and solutions should be channeled.

20.5.2 Mass Education

The purpose of mass education is to involve as many people as possible with limited resources and maximum effect. The methods to achieve this are usually through community involvement through community-based activities such as charity walks and other sports-related activities. Using an army of volunteers to organize local, regional, and national activities, the approach similar to that of common causes such as AIDS, cancer, and other life-threatening diseases, can bring quick and very effective awareness which leads to unprecedented education.

20.6 Reporting Centers

The recent skyrocketing rise in cyber crimes has prompted public authorities looking after the welfare of the general public to open up cyber crime reporting centers.

The purpose of these centers is to collect all relevant information on cyber attacks and make that information available to the general public. The centers also function as the first point of contact whenever one suspects or is electronically attacked. Centers also act as advice-giving centers for those who want to learn more about the measures that must be taken to prevent, detect, and recover from attacks, and in a limited capacity, these centers offer security education.

In the United States, there are several federally supported and private reporting centers, including NIST Computer Security Division:

Computer Security Resource Center (CSRC) (http://csrc.nist.gov/)
The Department of Homeland Security (DHS)'s National Cybersecurity and Communications Integration Center (NCCIC) (http://www.dhs.gov/national-cybersecurity-and-communications-integration-center)
The Center for Education and Research in Information Assurance and Security (https://www.cerias.purdue.edu/)
Carnegie Mellon Emergency Response Team (https://www.cert.org/about/)
The FedCIRC (http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Security/DEV01_003675)
The National Infrastructure Protection Center (https://www.dhs.gov/national-infrastructure-coordinating-center)

These centers fall into two categories:

- Non-law enforcement to collect, index, and advise the population of all aspects of cyber attacks including prevention, detection, and survivability.
- Law enforcement centers to act as the nation's clearing house for computer crimes, linking up directly with other national and international Computer Emergency Response Teams to monitor and assess potential threats. In addition, law enforcement centers may provide training for local law enforcement officials and in cooperation with private industry and international law enforcement agencies.

20.7 Market Forces

The rapid rise in cyber crimes has also prompted collaboration between private industry and government agencies to work together to warn the public of the dangers of cyber crimes and outline steps to take to remove the vulnerabilities, thereby lessening chances of being attacked. Both major software and hardware manufacturers have been very active and prompt in posting, sending, and widely distributing advisories, vulnerability patches, and antivirus software whenever their products are hit. Cisco, a major Internet infrastructure network device manufacturer, for example, has been calling and e-mailing its customers worldwide, mainly Internet service providers (ISPs), notifying them of the possibilities of cyber attacks that target Cisco's products. It also informs its customers of software patches that could be used to resist or repair those attacks. It has also assisted in the dissemination of vital information to the general public through its Web sites concerning those attacks and how to prevent and recover from them.

On the software front, Microsoft, the most affected target in the software arena, has similarly been active in posting, calling, and e-mailing its customers with the vital and necessary information on how to prevent and recover from attacks targeting its products. Besides the private sector, public sector reporting centers have also been active in sending advisories of impending attacks and techniques to recover from attacks.

20.8 Activism

Beyond those awareness and mass education techniques discussed above, there are others widely used although less effective. They fall under the activism umbrella because they are organized and driven by the users. They include the following:

20.8.1 Advocacy

This is a mass education strategy that has been used since the beginning of humanity. Advocacy groups work with the public, corporations, and governments to enhance public education through awareness of the use. It is a blanket mass

education campaign in which a message is passed through mass campaigns, magazines, and electronic publications, as well as support of public events and mass communication media like television, radio, and now the Internet.

Advocacy is intended to make people part of the intended message. For example, during the struggles for the voting rights in the United States, women's groups and minorities designed and carried out massive advocacy campaigns that were meant to involve all women who eventually became part of the movement. Similarly, in the minority voting rights struggles, the goal was to involve all minorities whose rights had been trodden upon. The purpose of advocacy is to consequently organize, build, and train so that there is a permanent and vibrant structure that people can be part of. By involving as many people as possible including the intended audience in the campaigns, the advocacy strategy brings awareness which leads to more pressure on lawmakers and everyone else responsible. The pressure brought about by mass awareness usually results in some form of action, most times the desired action.

20.8.2 Hotlines

Hotlines is a technique that makes the general public take the initiative to observe, notice, and report incidents. In fact, as we will see in the next chapter, the *National Strategy to Secure Cyberspace* (NSSC), in one of its priorities, advocates this very strategy to make the ordinary users get involved in not only their personal security but also that of their community and the nation as a whole. In many cases, the strategy is to set up hotline channels through which individuals who observe a computer security incident can report it to the selected reporting agency for action. Whenever a report is made, any technique that works can be applied. In many countries such agencies may include their ISPs and law enforcement agencies.

Exercises

1. Do you think education can protect cyberspace from criminal activities? Defend your response.
2. Looking at the array of education initiatives and different types of programs and the state of security in cyberspace, do you think education can advance/improve system security?
3. The effects of education are not seen in a few years. In fact, education benefits may show 20–30 years later. However, security needs are for real and for now. Should we keep educating?
4. Choose three hardware solutions used in self-regulation and discuss how they are deployed and how they work.
5. Choose three software solutions based on self-regulation. Study the solutions and discuss how they work.
6. Study the various forms of activism. Comment on the effectiveness of each.

7. Software rating, although helpful in bringing awareness to concerned individuals, has not been successful. Discuss why.
8. Both blocking software and filtering software, although slightly more popular than rating software, suffer from a variety of problems. Discuss these problems and suggest solutions.
9. Given that worldwide a small percentage of people have college education, but, in some countries, more than half of the people use computers and get access to cyberspace, propose a way to get your education message to those people who may not have enough education to understand the computer lingo. Discuss how much of the computer lingo is a problem in mass education.
10. Information security awareness and education are effective if people do understand the lingo used. Computer technology has generated a basket of words that make it difficult for an average computer user to benefit fully from either vendor education or specialized education. Suggest ways to deal with the ever-expanding basket in computer and information security.

Advanced Exercises

1. Study five countries with strong laws on cyberspace activities, and comment on these laws' effectiveness.
2. One of the problems of cyberspace regulation is the hindrance to hot pursuit of cyber criminals. Hot pursuit laws prevent law enforcement officers from crossing jurisdictional boundaries without court permissions. However, digital evidence does not give you that much time to collect court permits. Discuss these problems and suggest ways to overcome them.
3. Study the big market players, both hardware and software, and discuss their efforts in bringing security awareness to their customers. Are they being noble or responding to pressure?
4. As a follow up to question #3 above, if there was more competition on the market, do you think there would be more security responsibility? Why or why not?
5. If possible, propose a unique education security solution that is not among those discussed. Give reasons why your solution might succeed where others have fallen short.

Reference

1. Committee to Study High Performance Computing and Communications (1995) Evolving the high performance computing and communications initiative to support the nation's information infrastructure. The National Academies Press, Washington, DC. http://www.nap.edu/readingroom/books/hpcc/contents.html