Ethical, Privacy, and Security Issues in the Online Social Network Ecosystems

13

Learning Objectives

After reading this chapter, the reader should be able to:

1. Understand computer networks
2. Understand social networks
3. Understand online social networks
4. Understand privacy issues affecting online social networks
5. Discuss privacy issues in social networks
6. Discuss ethical issues in online social networks
7. Discuss the security issues in online social networks
8. Discuss the limitations of legislation network to deal with online social, privacy, and security issues

13.1 Introduction

Because we intend to focus on online social networks in this chapter, it is imperative that the reader gets a good grasp of network infrastructure upon which the online social network is anchored. So we will start this chapter with a light introduction of the concepts of a computer network. Some knowledge of the computer network infrastructure will help the reader understand how these online social network services, discussed in Sect. 13.4.3, work. So here is a soft introduction to computer networks.

Definition: An ecosystem is a localized group of interdependent organisms together with the environment that they inhabit and depend on.

J.M. Kizza, *Ethical and Social Issues in the Information Age*, Texts in Computer Science,
DOI 10.1007/978-1-4471-4990-3_13,

13.2 Introduction to Computer Networks

A *computer network* is a distributed system consisting of loosely coupled computing elements and other devices. In this configuration, any two of these devices can communicate with each other through a communication medium. The medium may be wired or wireless. To be considered a communicating network, the distributed system must communicate based on a set of communicating rules called *protocols*. Each communicating device in the network must then follow these rules to communicate with others. A standard wired computer network would look like the network in Fig. 13.1.

Individually, network elements may own resources that are local or global. Such resources may be either software-based or hardware-based. If software, it may consist of all application programs and network protocols that are used to synchronize, coordinate, and bring about the sharing and exchange of data among the network elements. Network software also makes the sharing of expensive resources in the network possible. The hardware components of a computer network consist of a collection of nodes that include the end systems commonly called *hosts* and intermediate switching elements that include hubs, bridges, routers, and gateways.

13.2.1 Computer Network Models

Several network configuration models are used in the design of computer networks, but the most common are two: the centralized and distributed models shown in Figs. 13.2 and 13.3. In a centralized model, all computers and devices in the network are connected directly to a central computer, through which they can interconnect to

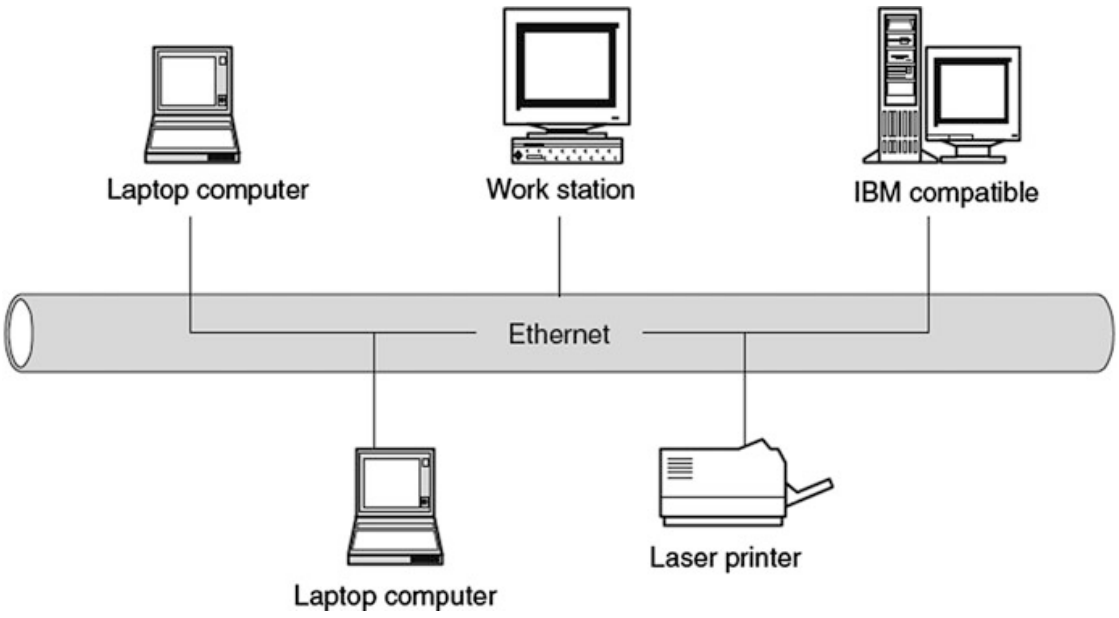

Fig. 13.1 A computer network

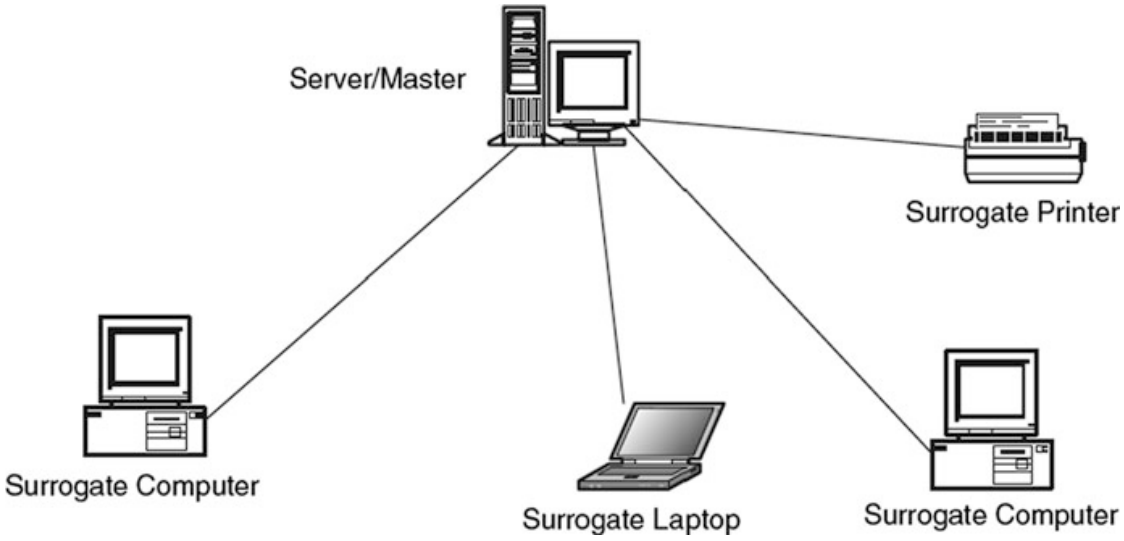

Fig. 13.2 A centralized network model

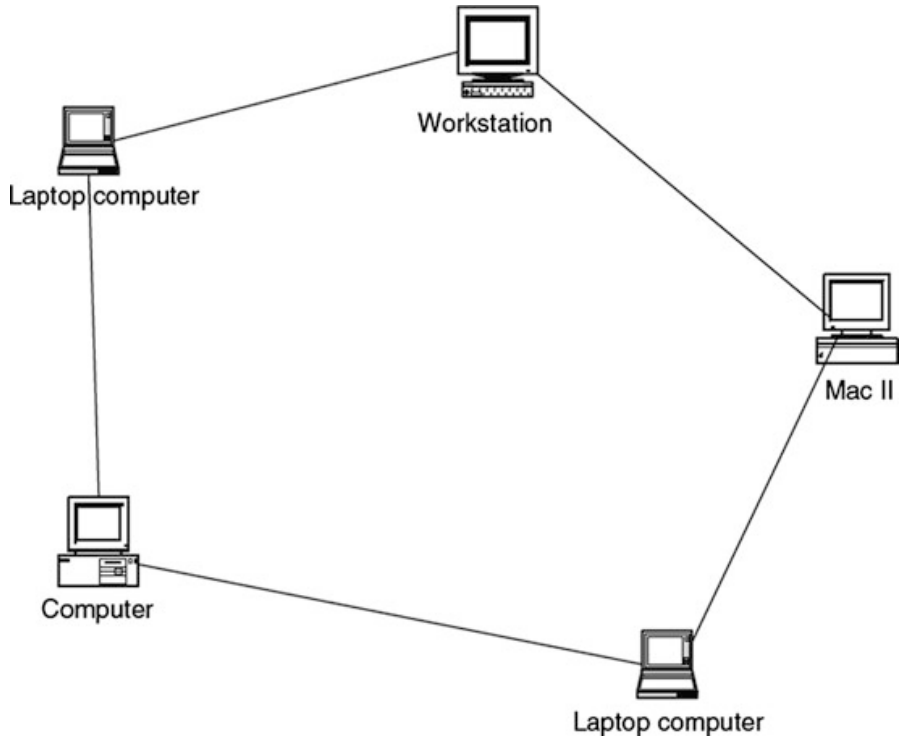

Fig. 13.3 A distributed network model

each other. This central computer, commonly called the master, must receive and forward all correspondence between any two or more communicating computers and devices. All other computers in the network are correspondently called dependent or surrogate computers. These surrogates may have reduced local resources, such as memory, and shareable global resources are controlled by the master at the center. The configurations are different, however, in the distributed network model. This

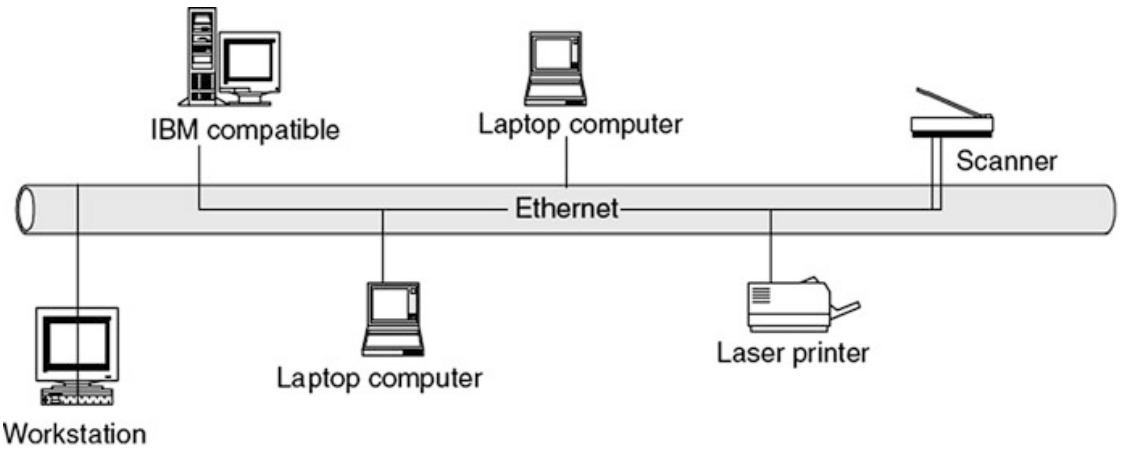

Fig. 13.4 A LAN network

consists of loosely coupled computers interconnected by a communication network consisting of connecting elements and communication channels. However, unlike in the centralized model, here the computers themselves may own their own resources locally or may request resources from a remote computer. Computers in this model are known by a string of names, including host, client, or node.

13.2.2 Computer Network Types

Computer networks, in any configuration centralized or distributed, come in different sizes depending on the number of computers and other devices the network has. The number of devices, computers or otherwise, in a network and the geographical area covered by the network determine the network type. There are, in general, three main network types: the local area network (LAN), a wide area network (WAN), and metropolitan area network (MAN).

13.2.2.1 Local Area Network

A LAN is a computer network with two or more computers or clusters of network and their resources connected by a communication medium sharing communication protocols and confined in a small geographical area such as a building floor, a building, or a few adjacent buildings. In a LAN, all network elements are in close proximity, which makes the communication links maintain a higher speed and quality of data movement. Figure 13.4 shows a LAN.

13.2.2.2 Wide Area Network

A WAN is a computer network made up of one or more clusters of network elements and their resources, but unlike in the LAN, here, the configuration is not confined to a small geographical area. It can spread over a wide geographical area like a region of a country, or across the whole country, several countries, or the entire globe like

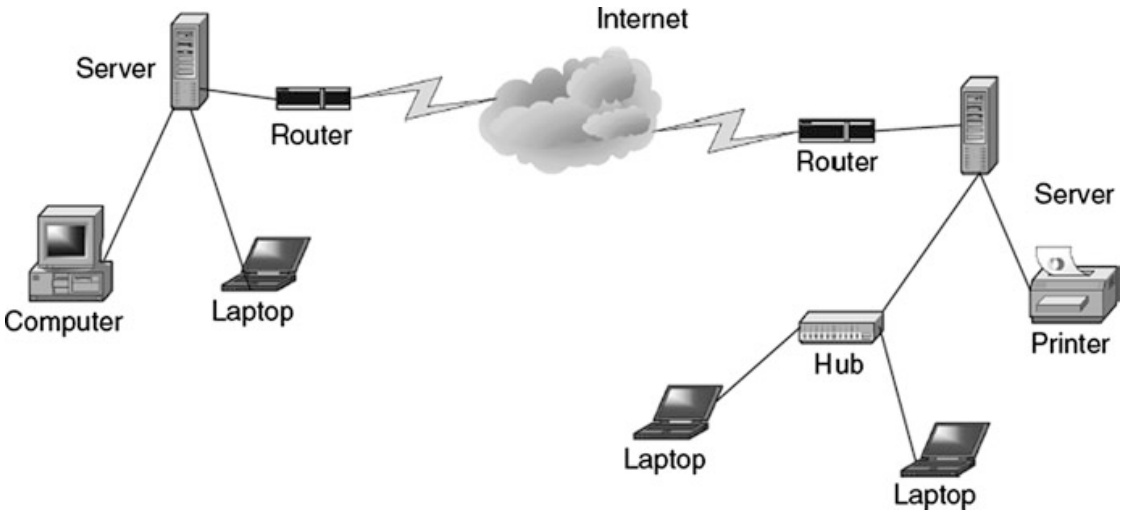

Fig. 13.5 A WAN network

the Internet, for example, which helps in distributing network services and resources to a wider community. Figure 13.5 shows a WAN.

13.2.2.3 Metropolitan Area Network

A metropolitan area network (MAN) is an unusual and less used type of a network that falls between a LAN on the one side and a WAN on the other. It covers a slightly wider area than the LAN but not so wide as to be considered a WAN. Civic networks that cover a city or part of a city are a good example of a MAN.

13.2.2.4 Mesh Network

A mesh network topology allows multiple access links between network elements, unlike other types of network topologies. The multiplicity of access links between network elements offers an advantage in network reliability because whenever one network element fails, the network does not cease operations; it simply finds a bypass to the failed element, and the network continues to function. The mesh network topology is most often applied in metropolitan area networks (MANs), also known as civic networks that cover a city or part of a city. Figure 13.6 shows a mesh network.

13.3 Social Networks (SNs)

A *social network* is a theoretical network where each node is an individual, a group, or organization who independently generates, captures, and disseminates information and also serves as a relay for other members of the network. This means that individual nodes must collaborate to propagate the information in the network. The links between nodes represent relationships and social interactions between individuals, groups, organizations, or even entire societies.

The concept of social networking is not new. Sociologists and psychologists have been dealing with and analyzing social networks for generations. In fact, social

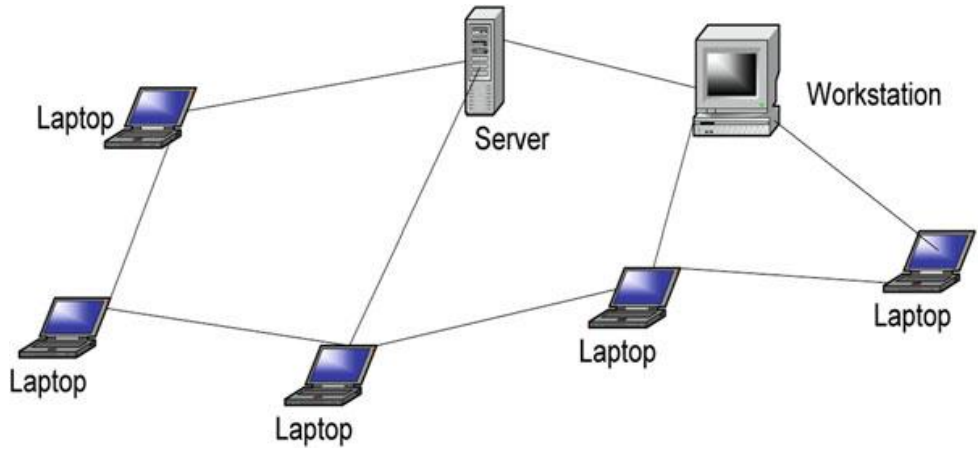

Fig. 13.6 Mesh network

networks have been in existence since the beginning of man. Prehistoric man formed social networks for different reasons including security, access to food, and the social well-being.

Social networks begin with an individual reaching out to another individual or group for a social relationship of sorts, and it snowballs into a mesh of social relationships connecting many individuals and/or groups. In general, social networks come in all sizes and are self-organizing, complex, and agile depending on the nature of relationships in its links. As they grow in size, social networks tend to acquire specific elements and traits that make them different. These traits become more apparent as the network size increases. The type of social interactions, beliefs, and other traits usually limit the size of the social network. It is important to note that as the social network grows big, it tends to lose the nuances of a local system; hence, if certain qualities of the network properties are needed, it is better to keep the size under control. Figure 13.7 illustrates three stages of development of a social network as it grows.

13.4 Online Social Networks (OSNs)

Online social networks (OSNs) are social networks with underlining electronic communication infrastructure links enabling the connection of the interdependencies between the network nodes. The discussion in this chapter will focus on these OSNs. In particular, we will focus on two types of online social networks:

- The traditional OSNs such as Facebook and MySpace. Many of these can be accessed via mobile devices without the capability of dealing with mobile content.
- The Mobile OSNs (mOSNs) which are newer OSNs that can be accessed via mobile devices and can deal with the new mobile context.

The interdependency between nodes in the OSNs supports social network services among people as nodes. These interdependencies as relations among people participating in the network services define the type of OSNs.

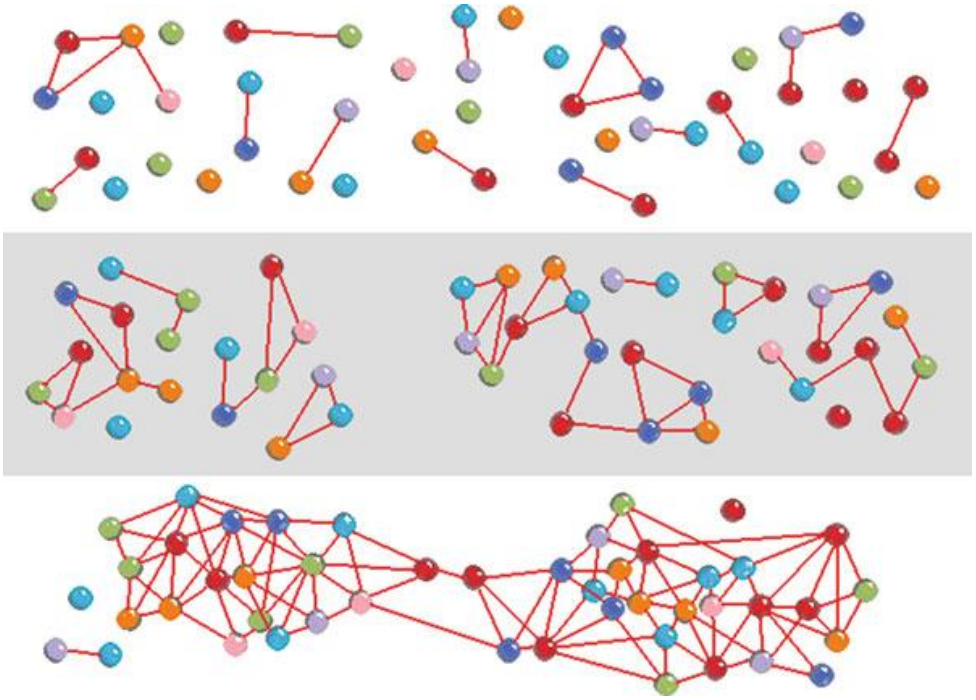

Fig. 13.7 Social network self-organizing configurations (http://en.wikipedia.org/wiki/File:Network_self-organization_stages.png)

13.4.1 Types of Online Social Networks

The growth of the OSNs over the years since the beginning of digital communication saw them evolving through several types. Let us look at the most popular types using a historical chronology.

Chat Network. The chat network was born out of the digital chatting anchored on a *chat room*. The chat room was and still is a virtual room online where people "gather" just to chat. Most chat rooms have open access policies meaning that anyone interested in chatting or just reading others' chats may enter the chat room. People can "enter" and "exit" any time during the chats. At any one time, several threads of the public chats may be going on. Each individual in the chat room is given a small window on his or her communication device to enter a few lines of chat contributing to one or more of the discussion threads. This communication occurs in real time, and whatever every one submits to the chat room can be seen by anyone in the chat room. Chat rooms also have a feature where a participating individual can invite another individual currently in the public chat room into a private chat room where the two can continue with limited "privacy." To be a member of the chat room, you must create a username, and members of the chat room will know you by that. Frequent chatters will normally become acquaintances based on usernames. Some chat room software allows users to create and upload their profiles so that users can know you more via your profile.

Although chat rooms by their own nature are public and free for all, some are monitored for specific compliance based usually on attributes like topics under discussion.

With the coming of more graphical-based online services, the use of chat room is becoming less popular especially to youth.

Blog Network. Another online social network is the bloggers network. "Blogs" are nothing more than people's online journals. Avid bloggers keep diaries of daily activities. These diaries sometimes are specific on one thread of interest to the blogger or a series of random logs of events during a specific activity. Some blogs are comment on specific topics. Some bloggers have a devoted following depending on the issues.

Instant Messaging Network (IMN). The IMN support real-time communication between two or more individuals. Like chat rooms, each participant in the IM must have a username. To IM an individual, one must know that individual's username or screen name. The initiator of the IM is provided with a small window to type the message, and the recipient is also provided with a similar window to reply to the message. The transcript of the interchange is kept scrolling up both users' screens. Unlike the chat room, however, these exchanges of short messages are private. Like in chat networks, some IMN allow users to keep profiles of themselves.

Online Social Networks (OSNs). These are a combination of all the network types we have discussed above and other highly advanced online features with advanced graphics. There are several of these social networks including Facebook, Twitter, Myspace, Friendster, YouTube, Flickr, and LinkedIn. Since these networks grew out of those we have seen before, many of the features of these networks are those we have discussed in the above networks. For example, users in these networks can create profiles that include their graphics and other enclosures and upload them to their network accounts. They must have a username or screen name. Also communication, if desired, can occur in real time as if one is using chat or IM capabilities. In addition to real time, these networks also give the user the delayed and archiving features so that the users can store and search for information. Because of these additional archival and search capabilities, network administrators have fought with the issues of privacy and security of users as we will see later in this chapter. As a way to keep users data safe, profiles can be set to a private setting, thus limiting access to private information by an authorized users.

13.4.2 Online Social Networking Services

An online social networking service is an online service accessible via any Internet-enabled device with the goal of facilitating computer-mediated interaction among people who share interests, activities, backgrounds, or real-life connections. Most online social network services consist of:

- User profile
- Social or business links of interests
- Additional services

Currently, the most popular online social network services fall in categories that range from friends-based, music and movie, religion, business, and many other interests. In each of these categories, let us give a sample of the current services:

- General and friends-based social networks
  - Facebook

  - MySpace
  - Hi5
- Movie and music social networks
  - LastFM
  - Flixster
  - iLike
- Mobile social networks
  - Dodgeball
  - Loopt
  - Mozes
- Hobby and special interest social networks
  - ActionProfiles
  - FanIQ
- Business social networks
  - LinkedIn
  - XING
  - Konnects
- Reading and books social networks
  - GoodReads
  - Shelfari
  - LibraryThing

13.4.3 The Growth of Online Social Networks

OSNs have blossomed as the Internet exploded. The history and the growth of OSNs have mirrored and kept in tandem with the growth of the Internet. At the infant age of the Internet, computer-mediated communication services like Usenet, ARPANET, LISTSERV, and bulletin board services (BBS) helped to start the growth of the current OSNs as we know them today. Let us now see how these contributed to the growth of OSNs.

BITNET was an early world leader in network communications for the research and education communities and helped lay the groundwork for the subsequent introduction of the Internet, especially outside the USA [1]. Both BITNET and Usenet were invented around the same time in 1981 by Ira Fuchs and Greydon Freeman at the City University of New York (CUNY), where both "store-and-forward" networks were. BITNET was originally named for the phrase "Because It's There Net," later updated to "Because It's Time Net" [1]. It was originally based on IBM's VNET *e-mail* system on the IBM virtual machine (VM) mainframe operating system. But it was later emulated on other popular operating systems like DEC VMS and *Unix*. What made BITNET so popular was its support of a variety of mailing lists supported by the *LISTSERV* software [2].

BITNET was updated in 1987 to BITNET II to provide a higher bandwidth network similar to the *NSFNET*. However, by 1996, it was clear that the Internet was providing a range of communication capabilities that fulfilled BITNET's roles, so CREN ended their support and the network slowly faded away[2].

Bulletin Board Services (BBS). A bulletin board system (BBS) is a software running on a computer allowing users on computer terminals far away to login and access the system services like uploading and downloading files and reading news and contribution of other members through e-mails or public bulletin boards. In "Electronic Bulletin Boards, A Case Study: The Columbia University Center for Computing Activities," Janet F. Asteroff [3] reports that the components of computer conferencing that include private conferencing facilities, electronic mail, and electronic bulletin boards started earlier than the electronic bulletin board (BBS). Asteroff writes that the concept of an electronic bulletin board began c. 1976 through ARPANET at schools such as the University of California at Berkeley, Carnegie-Mellon, and Stanford University. These electronic bulletin boards were first used in the same manner as physical bulletin boards, that is, help wanted, items for sale, public announcements, and more. But electronic bulletin boards soon became, because of the ability of the computer to store and disseminate information to many people in text form, a forum for user debates on many subjects. In its early years, BBS connections were via telephone lines and modems. The cost of using them was high; hence, they tended to be local. As the earlier form of the World Wide Web, BBS use receded as the World Wide Web grows.

LISTSERV. It started in 1986 as an automatic mailing list server software which broadcasts e-mails directed to it to all on the list. The first LISTSERV was conceived of by Ira Fuchs from *BITNET* and Dan Oberst from EDUCOM (later EDUCAUSE) and implemented by Ricky Hernandez also of EDUCOM, in order to support research mailing lists on the *BITNET* academic research network [4].

By the year 2000, LISTSERV ran on computers around the world managing more than 50 thousand lists, with more than 30 million subscribers, delivering more than 20 million messages a day over the Internet [4].

Other Online Services. As time went on and technology improved, other online services come along to supplement and always improve on the services of whatever was in use. Most of the new services were commercially driven. Most of them were moving toward and are currently on the Web. These services including news, shopping, travel reservations, and others were the beginning of the Web-based services we are enjoying today. Since they were commercially driven, they were mostly offered by ISPs like AOL, Netscape, Microsoft, and the like. As the Internet grew, millions of people flocked onto it, and the Web and services started moving away from ISP to fully fledged online social network companies like Facebook, Flicker, Napster, Linked, Twitter, and others.

13.5 Ethical and Privacy Issues in Online Social Networks

Privacy is a human value consisting of a set of rights including solitude, the right to be alone without disturbances; anonymity, the right to have no public personal identity; intimacy, the right not to be monitored; and reserve, the right to control one's

personal information, including the dissemination methods of that information. As humans, we assign a lot of value to these four rights. In fact, these rights are part of our moral and ethical systems. With the advent of the Internet, privacy has gained even more value as information has gained value. The value of privacy comes from its guardianship of the individual's personal identity and autonomy.

Autonomy is important because humans need to feel that they are in control of their destiny. The less personal information people have about an individual, the more autonomous that individual can be, especially in decision making. However, other people will challenge one's autonomy depending on the quantity, quality, and value of information they have about that individual. People usually tend to establish relationships and associations with individuals and groups that will respect their personal autonomy, especially in decision making.

As information becomes more imperative and precious, it becomes more important for individuals to guard their personal identity. Personal identity is a valuable source of information. Unfortunately, with rapid advances in technology, especially computer and telecommunication technologies, it has become increasingly difficult to protect personal identity.

13.5.1 Privacy Issues in OSNs

Privacy can be violated, anywhere including in online social network communities, through intrusion, misuse of information, interception of information, and information matching [5]. In online communities, intrusion, as an invasion of privacy, is a wrongful entry, a seizing, or acquiring of information or data belonging to other members of the online social network community. Misuse of information is all too easy. While online, we inevitably give off our information to whomever asks for it in order to get services. There is nothing wrong with collecting personal information when it is authorized and is going to be used for a legitimate reason. Routinely, information collected from online community members, however, is not always used as intended. It is quite often used for unauthorized purposes, hence an invasion of privacy. As commercial activities increase online, there is likely to be stiff competition for personal information collected online for commercial purposes. Companies offering services on the Internet may seek new customers by either legally buying customer information or illegally obtaining it through eavesdropping, intrusion, and surveillance. To counter this, companies running these online communities must find ways to enhance the security of personal data online.

As the number and membership in online social networks skyrocketed, the issues of privacy and security of users while online and the security of users' data while off-line have taken center stage. The problems of online social networking have been made worse by the already high and still growing numbers especially of young people who pay little to no attention to privacy issues for themselves or others. Every passing day, there is news about and growing concerns over breaches in privacy caused by social networking services. Many users are now worried that their

personal data is being misused by the online service providers. All these privacy issues can be captured as follows [6]:

- Sharing of personal information with all OSN users:
  - Users in the network give out too much personal information without being aware who might wrongly use that information. Sexual predators are known to use information from teens on these networks. Currently, many of the OSNs are working with law enforcement to try to prevent such incidents [5]. Information such as street address, phone number, and instant messaging name are routinely disclosed to an unknown population in cyberspace.
  - Ease of access to OSNs. Currently, it is very easy for anyone to set up an account on anyone of these networks with no requirements to specific identifications. This can lead to identity theft or impersonation [5].
  - Privacy threat resulting from placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken [5].
  - Updating profiles with current activities poses a great threat, for example, updating your profile informing people of your whereabouts.
- Lack of precise rules by the OSNs on who should use which data.
- Leakage of private information to third parties:
  - On many of these networks, information altered or removed by a user may in fact be retained and/or passed to third parties [5].
- Inter-linkages in OSNs. In their paper "(Under)mining Privacy in Social Networks," Monica Chew, Dirk Balfanz, and Ben Laurie of Google, Inc., point to three distinct areas where the highly interlinked world of social networking sites can compromise user privacy. They are [7]:
  - Lack of control over activity streams: An *activity stream,* according to the authors, is a collection of events associated with a single user including changes a user makes to his or her profile page, the user adding or running a particular application on the social networking site, news items shared, or communication with friends. Activity streams may compromise a user's privacy in two ways:
    - A user may not be aware of all the events that are fed into their activity streams in which case the user lacks control over those streams.
    - A user may not be aware of the audience who can see their activity streams in which case the user lacks control over the audience who could see the activity stream.
  - Unwelcome linkage: *Unwelcome linkage* occurs when links on the Internet reveal information about an individual that they had not intended to reveal. Unwelcome linkage may occur wherever graphs of hyperlinks on the World Wide Web are automatically created to mirror connections between people in the real world. Maintaining separation of individual activities and different personae is important in OSNs.
  - De-anonymization of users through merging of social graphs. OSN sites tend to extract a lot of personally identifiable information from people such as

birth date and address. With this information, it is possible to deanonymize users by comparing such information across social networking sites, even if the information is partially obfuscated in each OSN.

As the growth in online social networks continues unabated, the coming in the mix of the smart mobile devices is making the already existing problems more complex. These new devices are increasing the number of accesses to OSNs and increasing the complexity of the privacy issues, including, in addition to those above in the traditional (OSNs) [8]:

- The presence of a user. Unlike in the most traditional OSNs where users were not automatically made aware of the presence of their friends, most mobile OSNs (mOSN) now allow users to indicate their presence via a "check-in" mechanism, where a user establishes their location at a particular time. According to Krishnamurthy and Wills [8], the indication of presence allows their friends to expect quick response, and this may lead to meeting new people who are members of the same mOSN. Although the feature of automatic locate by oneself is becoming popular, it allows leakage of personal private information along two tracks: the personal information that may be sent and the destination to which it could be sent.
- Location-based tracking system (LTS) technologies that are part of our mobile devices. This is a feature that is widespread in the mobile environment. However, users may not be aware that their location can be made known to friends and friends of friends who are currently online on this mOSN, their friends in other mOSNs, and others may lead to leakage of personal information to third parties.
- Interaction potential between mOSNs and traditional OSNs. According to Krishnamurthy and Wills [8], such connections are useful to users who, while interacting with a mOSN, can expect some of their actions to show up on traditional OSNs and be visible to their friends there. However, a lot of their personal information can leak to unintended users of both the traditional OSNs and the mOSNs.

In addition to almost free access to a mountain of personal data on OSNs, there is also a growing threat to personal data ownership, for example, who owns the data that was altered or removed by the user which may fact be retained and/or passed to third parties. This danger was highlighted when in June 2011, a 24-year-old Austrian law student, Max Schrems, asked Facebook for a copy of all his personal data. Facebook complied, sending him a CD containing 1,200 pages of data, including his likes, "friend" and "defriend" history, and chat logs. But before that, Schrems had deleted some of the data returned to him from his profile, yet Facebook had retained his information. Of course Schrems filed 22 individual claims against Facebook for €100,000 ($138,000) for retaining data deleted by users in the case *Europe vs. Facebook* [9].

Fortunately, users are beginning to fight for their privacy to prevent their personal details from being circulated far widely than they intended it to be.

Since online social networks, just like their predecessor cyberspace communities are bringing people together with no physical presence to engage in all human acts

that traditionally have taken place in a physical environment that would naturally limit the size of the audience and the amount of information given at a time. As these cybercommunities are brought and bound together by a sense of belonging, worthiness, and the feeling that they are valued by members of the network, they create a mental family based on trust, the kind of trust you would find in a loving family. However, because these networks are boundaryless and international in nature, they are forming not along well-known and traditional identifiers such as nationalities, beliefs, authority, and the like but by common purpose and need with no legal jurisdiction and no central power to enforce community standards and norms.

13.5.2 Strengthening Privacy in OSNs

As more and more people join OSNs and now the rapidly growing mOSNs, there is a growing need for more protection to users. Chew et al. suggest the following steps needed to be taken [7]:

- Both OSN and mOSN applications should be explicit about which user activities automatically generate events for their activity streams.
- Users should have control over which events make it into their activity streams and be able to remove events from the streams after they have been added by an application.
- Users should know who the audience of their activity streams is and should also have control over selecting the audience of their activity streams.
- Both OSN and mOSN application should create activity stream events which are in sync with user expectation.

Other suggestions that may help in this effort are:

- Use secure passwords.
- User awareness of the privacy policies and terms of use for their OSNs and mOSNs.
- Both OSNs and mOSNs providers should devise policies and enforce existing laws to allow some privacy protection for users while on their networks.

13.5.3 Ethical Issues in Online Social Networks

Online social communities including online social network are far from the traditional physical social communities with an epicenter of authority with every member paying allegiance to the center with a shared sense of responsibility. This type of community governance with no central command, but an equally shared authority and responsibility, is new, and a mechanism needs to be in place and must be followed to safeguard every member of the community. But these mechanisms are not yet defined, and where they are being defined, it is still too early to say

whether they are effective. The complexity, unpredictability, and lack of central authority are further enhanced by:

- *Virtual personality*: You know their names, their likes, and dislikes. You know them so well that you can even bet on what they are thinking, yet you do not know them at all. You cannot meet them and recognize them in a crowd.
- *Anonymity*: You work with them almost every day. They are even your friends; you are on a first-name basis, yet you will never know them. They will forever remain anonymous to you and you to them.
- *Multiple personality*: You think you know them, but you do not because they are capable of changing and mutating into other personalities. They can change into as many personalities as there are issues being discussed. You will never know which personality you are going to deal with next.

These three characteristics are at the core of the social and ethical problems in online social networks in particular and cyberspace in general; the larger and more numerous these communities become, the more urgent the ethical concerns become. With all these happening in online social network, the crucial utilitarian question to ask is what is best way and how can we balance the potential harms and benefits that can befall members of these online social networks and how if possible to balance these possibilities. Of late, the news media has been awash with many of these online ills and abuses, and the list is growing including:

1. *Potential for misuse*
   Online social networks offer a high degree of freedom which is being misused by a growing number of users. Cases are abound of these incidents with tragic endings including suicide, especially in young people.
2. *Cyberbullying, cyberstalking, and cyber-harassment*
   Cyberbullying, cyberstalking, and electronic harassment are relatively common occurrence and can often result in emotional trauma for the victim. But they are unfortunately becoming a common form of abuse on online social network sites like Facebook and MySpace, especially to youth. Cyberbullying is defined as use of Internet services and mobile technologies such as Web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person. Cyberstalking or cyber-harassment on the other hand is defined as the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass [10].

   Because of the nature of cyberspace's telepresence, anonymity, lack of allegiance of users, and nonexistence of central governance, there are no limitations as to what individuals can post when online and to what degree of toxicity those posts can be. Individuals, therefore, take it as if they are given the power to post offensive remarks or pictures that could potentially cause a great amount of emotional pain oftentimes leading to teen suicide. Cases are

growing of these kinds of activities, some of which are tragic. Bullying statistics show that cyberbullying is a serious problem alarmingly common among adolescents and teens. According to cyberbullying statistics from the i-SAFE foundation [11]:

- Over half of adolescents and teens have been bullied online, and about the same number have engaged in cyberbullying.
- More than 1 in 3 young people have experienced cyberthreats online.
- Over 25 % of adolescents and teens have been bullied repeatedly through their cell phones or the Internet.
- Well over half of young people do not tell their parents when cyberbullying occurs.

As these statistics indicate, the number of teen suicide due to cyberbullying is on the rise.

3. *Risk for child safety*
   Problems with online social networks are not only limited to misuse of the sites and cyberbullying; they also include real threat to children whether cyberbulled or not. There is growing exploitation of children in online social networks. Latest figures show that around one million children under 16 use Bebo, while 600,000 minors are on MySpace [12]. With these numbers, the potential for child abuse online is growing. The networking sites say they are making it possible for users to report abuse, though those reports usually go to the site administrators rather than the authorities. Governments around the world are taking steps, at least to better understand the problem and find some solutions.
   Discussion topics:
   - How do we balance these harms and benefits, reducing one and increasing the possibility of the other?
   - How do we protect individuals and how do we deal with the issue of consent?
4. *Psychological effects of online social networking*
   The rise in the use and membership of online social networking has resulted in the dramatic rise not only in the numbers of online social networks but also the number of users. Also with the rise in the number of users comes with the rise in the number of users with problems. More and more people, especially teens, are spending an excessive amount of time on the Internet in general and social networking sites in reality. This has led researchers to classify Internet addiction as a new clinical disorder [13].

   According to Neville Misquittaa in "Psychiatry and Society in Pune," the most common predictors of excessive use of social networking are [14]:

   - *Extroverted and unconscientious* individuals who spend more time on social networking sites, and their usage tends to be addictive.
   - *Shy people* also like Facebook and spend more time on it. However, they have few Facebook "friends."
   - *Narcissistic personalities* also have high levels of online social activity. They are recognized online by the quantity of their social interactions, their main photo self-promotion, and attractiveness of their main photo.

5. *Free speech*
   What types of speech are protected once one is in an online social network? Although the *National Labor Relations Act* protects workers from being fired for "protected concerted activity," which prevents workers from being fired for collective action, while allowing companies the right to fire workers for individual actions they take against the company, when it comes to online social networking, the issues are still murky, and there is still uncertainty as to the boundaries of what types of speech is protected in online social networks. This fuzziness is illustrated by the Pembroke Pines Charter High School case in which Katherine Evans, who was a senior at Pembroke Pines Charter High School in Florida in 2007, created a group on Facebook called "Ms. Sarah Phelps is the worst teacher I've ever met."

   Peter Bayer, the principal of Pembroke Pines High, suspended Evans for 3 days and removed her from her Advanced Placement classes for violating the school's rules against "cyberbullying" and "harassment" of a staff member, according to court documents. Evans sued the principal in his individual capacity, alleging that her First Amendment free speech and 14th Amendment due process rights were violated.

   In a ruling that followed, in *Bayer v. Evans*, US Magistrate Judge Barry L. Garber of Miami declined Evans's request for an injunction barring the principal from keeping the student's discipline in school records. But the judge denied qualified immunity for Bayer, holding that Evans's speech was protected under the First Amendment and that the principal should have known he was violating a clearly established right by disciplining Evans [15].

   This ruling, like is other recent rulings, speaks volumes about the ethics of social networking and schools, and it is indicative of the haziness of the legal boundaries of free speech in online social networks.

   Discussion topics: Should teachers be allowed to befriend students on sites such as Facebook? Should students blog about their teachers while on an online social network?

13.6 Security and Crimes in Online Social Networks

Online crimes, in tandem with the growth of computing and telecommunication technologies, are one of the fastest growing types of crimes, and they pose the greatest danger to online communities, e-commerce, and the general public in general. An *online crime* is a crime like any other crime, except that in this case, the illegal act must involve either an Internet-enabled electronic device or computing system either as an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime. Also online crimes are acts of unauthorized intervention into the working of the telecommunication networks and/or the sanctioning of authorized access to the resources of the computing elements in a network that lead to a threat to the system's infrastructure or cause a significant property loss. The

International Convention on Cybercrimes and the European Convention on Cybercrimes both list the following crimes as online crime [16]:

- Unlawful access to information
- Illegal interception of information
- Unlawful use of telecommunication equipment
- Forgery with use of computer measures
- Intrusions of the Public Switched and Packet Network
- Network integrity violations
- Privacy violations
- Industrial espionage
- Pirated computer software
- Fraud using a computing system
- Internet/e-mail abuse
- Using computers or computer technology to commit murder, terrorism, pornography, and hacking

13.6.1 Beware of Ways to Perpetuate Crimes in Online Social Networks

As we pointed out in Chap. 9, if we have to fight online crimes, we have to first learn how they are perpetuated. Earlier, we noted that online crimes are defined in a variety of ways. This reflects the many different ways these crimes are perpetuated. Some of the most common ways are through system penetration and denial of service attacks.

13.6.1.1 System Penetration

System penetration is the most widely used approach to committing online crimes. A system penetration is a process of gaining unauthorized access to a protected system's resources; the system may be automated or not. Penetration attacks always compromise the integrity of the resources of a system. Most penetration attacks are not accidental; they are preplanned and proceed with a coordinated reconnaissance. The goal of the reconnaissance is to acquire the following lead information on the targeted system:

- IP addresses of all hosts or selected hosts in the victim network
- Accessible UDP and TCP port numbers
- The type of operating system(s) used on all hosts or selected hosts in the network

There are two types of reconnaissance: passive and active. In a *passive reconnaissance*, the attacker gathers freely available system information mostly from open source. A typical passive reconnaissance can include physical observation of buildings housing the system and dumpster diving near the target system collecting discarded papers and system computer equipment in an attempt to find equipment or data that may include personal identifying data like username and passwords that will lead them to gain access to the company system. It also includes

using other information gathering techniques like eavesdropping on employee conversations, social engineering, packet sniffing, and others. Some common sources and tools used when looking for open source information legally include [17]:

- A company website
- Electronic data gathering, analysis, and retrieval (EDGAR) filings (for publicly traded companies)
- Network news transfer protocol (NNTP) USENET newsgroups
- User group meetings
- Business partners
- Dumpster diving
- Social engineering

Active reconnaissance on the other hand involves collecting information about a target system by probing that system or neighboring systems. A typical active reconnaissance involves port scanning to discover vulnerable ports through which to enter the system, probing firewalls and system routers to find ways around them, and others. Some of the tools used in active host reconnaissance include:

- NSLookup/Whois/Dig lookups
- SamSpade
- Visual Route/Cheops
- Pinger/WS_Ping_Pro

13.6.1.2 Distributed Denial of Service

Another approach perpetuators of online crimes use is the *denial of service*. This is an interruption of service of the target system. This interruption of service occurs when the target system is made either unavailable to users through disabling or destruction of it. Denial of service can also be caused by intentional degradation or blocking of computer or network resources. These denial of service attacks are commonly known as *distributed denial of service* (DDoS) attacks because they attack hosts in a network.

Like penetration attacks (e-attacks), DDoS attacks can also be either local, where they can shut down LAN computers, or global, originating thousands of miles away on the Internet. Attacks in this category include [16]:

- *IP spoofing*. A forging of an IP packet address such as the source address, which causes the responses from the destination host to be misdirected, thus creating problems in the network. Many network attacks are a result of IP spoofing.
- *SYN flooding*. Using a three-way handshake protocol to initiate connections between a malicious (spoofed) source nodes and flood the target node with so many connection requests thus overwhelming it and bringing it down.
- *Smurf attack*. In which the intruder sends a large number of spoofed ICMP Echo requests to broadcast IP addresses. Hosts on the broadcast multicast IP network then respond to these bogus requests with reply ICMP Echo significantly multiplying the number of reply ICMP Echo to the hosts with spoofed addresses.
- *Buffer overflow*. In which the attacker floods a carefully chosen field such as an address field with more characters than it can accommodate. These excessive

characters, usually executable malicious code, when executed, may cause havoc in the system, effectively giving the attacker control of the system.
- *Ping of death*. In which the attacker sends IP packets that are larger than the 65,536 bytes allowed by the IP protocol knowing that many network operating systems cannot handle, leading to the possible freezing or eventual system crash.
- *Land.c attack*. In which the land.c program sends TCP SYN packets whose source and destination IP addresses and port numbers are those of the victims.
- *Teardrop.c*. In which the attacker causes a fragmentation of TCP packets in order to exploit the reassembling process that may lead to the victim to crash or hang.
- *Sequence number sniffing*. In which the intruder takes advantage of the predictability of sequence numbers used in TCP implementations to sniff the next sequence number to establish legitimacy.

13.6.2 Defense Against Crimes in Online Social Networks

Although there are systems which are randomly attacked, most victim systems, however, are preselected for attack. Because of this, we can defend systems against online attacks. An effective defense plan consists of prevention, detection, and analysis and response.

13.6.2.1 Prevention

Prevention is perhaps the oldest and probably the best defense mechanism against online crimes. However, prevention can only work if there is a strict security discipline that is effectively enforced and must include the following:
- A security policy
- Risk management
- Vulnerability assessment
- Use of strong cryptographic algorithms
- Penetration testing
- Regular audits
- Use of proven security protocols
- Legislation
- Self-regulation
- Mass education

More details on some of these may be found in Sects. 5.3 and 8.3.

13.6.2.2 A Security Policy

A security policy is a critical and central document in an organization security efforts that spells out in great details how the organization manages risk, controls access to key assets and resources, and implements policies, procedures, and practices for a safe and secure environment [18]. A security policy usually also spells out what resources need to be protected and how organization can protect such resources. It is a living document and sometimes controversial. There are as many

opinions on the usefulness of security policies in the overall system security picture as there are security experts. However, security policies are still important in establishing an organization's security guidelines like:

- *Hardware and software acquisition and installations in the organization*. For example, if a functioning firewall is to be configured, its rule base must be based on a sound security policy.
- *User discipline*. All users in the organization who connect to a network, such as the Internet, must do so in conformity to the security policy.

A security policy is unique for each organization and covers a wide variety of topics and serves several important purposes in the organization's security cycle. Because of this, the following carefully chosen set of basic steps must be established and carefully followed in the construction of a viable implementable and useful security policy:

- Determining the resources that must be protected and for each resource drawing a profile of its characteristics
- Determining, for each identified resource, from whom the resource must be protected
- Determining, for each identifiable resource, the type of threat and the likelihood of occurrence of such a threat
- Determining, for each identifiable resource, what measures are needed to give it the best protection
- Determining what needs to be audited
- Determining and defining acceptable use of system resources such as e-mail, news, and Web
- Considering how to implement and deploy security protocols such as encryption, access control, key creation, and distributions and wireless devices that connect on the organization's network
- Providing for remote access to accommodate workers on the road and those working from home and also business partners who may need to connect to the organization's network via a VPN

13.6.2.3 Vulnerability Assessment

Like risk assessment, vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. A *vulnerability* in a system is an exploitable weakness in the system. As we saw in Sect. 8.3, this is a two-part process; we need to first identify all system vulnerabilities and then develop strategies to mitigate the effects of these vulnerabilities. The rest of the steps usually taken are similar to those in Sect. 8.3.

13.6.2.4 Use of Strong Cryptographic Algorithms

Cryptography is a Greek word meaning "secret writing." It was used to describe the art of secret communication. As shown in Figs. 5.1 and 13.8, cryptographic system consists of four essential components [16]:

- Plaintext—the original message to be sent
- A cipher—consisting of mathematical encryption and decryption algorithms

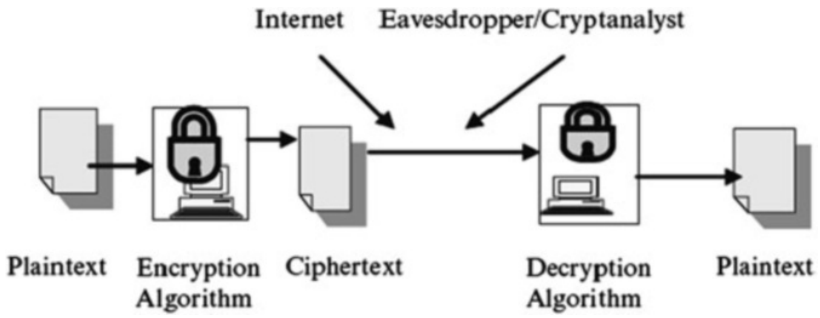

Fig. 13.8 Symmetric encryption

- Ciphertext—the result of applying an encryption algorithm to the original message before it is sent to the recipient
- Key—a string of bits used by the two mathematical algorithms in encrypting and decrypting processes

Cryptographic technologies are today being used increasingly to fight off massive invasion of individual privacy and security, to guarantee data integrity and confidentiality, and to bring trust in global e-commerce. In fact, cryptography has become the main tool for providing the needed digital security in the modern digital communication medium. Its popularity is a result of its ability to guarantee authorization, authentication, integrity, confidentiality, and nonrepudiation in all communications and data exchanges in the new information society.

13.6.2.5 Penetration Testing

One of the core security techniques for safeguarding the security of an organization's system is to periodically do a penetration test of the system. The test may be outsourced for it to be more authentic, or it could be carried out in-house as long as one has competent personnel to do it. The process of penetration testing actively evaluates an organization's system resources and information in real time looking for design weaknesses, technical flaws, and vulnerabilities in the system. This can be done on a regular basis or after a schedule time frame. The possible outcomes of the test vary depending on the focus of the test.

Penetration testing may also focus on the security of information on the organization network by doing tests like document grinding, privacy of information review, and intelligence scouting among others. If the organization supports wireless technology, this component must also be tested. No penetration testing can be complete without testing social engineering, communication within and outside the organization, and the physical security within the organization. Finally, physical testing may require testing access to the facilities, monitor the perimeter and alarm systems, and an environment review.

13.6.2.6 Regular Security Audits

While a penetration testing of an organization system is a focused look at the security holes in the system's resources such as firewalls and servers, a security audit is a systematic, measurable, and quantifiable technical assessment of the organization

security and the security of its system. Management usually requests for security audits in order to gain knowledge and understand the security status of the organization's system. From the audit report, management may decide to upgrade the system through acquisition of new hardware and software. In "Conducting a Security Audit: An Introductory Overview," Bill Hayes suggests that a security audit should answer the following questions [19]:

- Are passwords difficult to crack?
- Are there access control lists (ACLs) in place on network devices to control who has access to shared data?
- Are there audit logs to record who accesses data?
- Are the audit logs reviewed?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- Are these operating systems and commercial applications patched to current levels?
- How is backup media stored? Who has access to it? Is it up to date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind? How have these custom applications been tested for security flaws?
- How are configuration and code changes documented at every level? How are these records reviewed, and who conducts the review?

If genuine and trustful answers are given to many of these questions, a realistic security status of the organization's system emerges.

13.7 Proven Security Protocols and Best Practices in Online Social Networks

There are hundreds of security protocols to meet the needs of organizations trying to improve their systems' security. There are so many of them; some are open source, and others are not, that they pose a problem to security professionals to choose a really good product. The security personnel must strive to come up with a list of the best protocols and best practices to suit the system. Some of these protocols include the following.

13.7.1 Authentication

Authentication is the process of validating the identity of someone or something. It uses information provided to the authenticator to determine whether someone or something is in fact who or what it is declared to be. The process usually requires one to present credentials or items of value to the authenticating agent in order to

prove the claim of who one really is. The items of value or credential are based on several unique factors that show something you know, something you have, or something you are [16]:

- *Something you know*. It may be something you mentally possess like a password, a secret word known by the user and the authenticator. This technique of authentication is cheap but has weaknesses like memory lapses.
- *Something you have*. It may be any form of issued or acquired self-identification such as SecurID, ActivCard, or any other forms of cards and tags. This authentication technique is slightly safer.
- *Something you are*. These are individual physical characteristics such as voice, fingerprint, iris pattern, and other biometrics. Biometric authentication as we are going to see in Chap.14 is the safest form of authentication.

Besides these, there are other forms of authentication using a variety of authentication algorithms. These authentication methods can be combined or used separately, depending on the level of functionality and security needed. Among such methods are password authentication, public key authentication, anonymous authentication, and remote and certificate-based authentication.

13.7.2 Access Control

Access control is a process of determining how access to the system's potential resources can be provided to each of the system users. Because a system, especially a network system, may have thousands of users and resources, the management of access rights for every user per every object may become complex. Several control techniques and technologies have been developed to deal with this problem; they include access control matrix, capability tables, access control lists, role-based access control, rule-based access control, restricted interfaces, content-dependent access control, and biometrics.

13.7.3 Legislation

Ever since the start of noticeable computer technology misuse, governments and national legislatures around the world have been enacting laws intended to curb the growth of these crimes. The report card on these legislations has been mixed. In some cases, legislation as a form of deterrent has worked, and it has been a failure in others. However, we should not lose hope. Enforceable laws can be productive.

13.7.4 Self-Regulation

Perhaps one of the most successful forms of deterrence has been self-regulation. A number of organizations have formed to encourage parents and teachers to find a

way to regulate objectionable material from reaching the children. Also families and individuals, sometimes based on their morals and sometimes based on their religion, have made self-regulation a cornerstone of their efforts to stop the growing rate of online crimes.

13.7.5 Detection

While it is easy to develop mechanisms for preventing online crimes, it is not so easy to develop similar or effective techniques and best practices to detect online crimes. Detecting online crimes constitutes a 24-h monitoring system to alert security personnel whenever something unusual (something with a non-normal pattern, different from the usual pattern of traffic in and around the system) occurs. Detection systems must continuously capture, analyze, and report on the daily happenings in and around the network. In capturing, analyzing, and reporting, several techniques are used including intrusion detection, vulnerability scanning, virus detection, and other ad hoc methods.

13.7.6 Recovery

Recovery is a process preceded by the process of analysis, which involves taking as much data as possible gathered during the last intrusion and analyzing it for patterns that can be used in future for a response, for detection in future, and for prevention. Recovery requires the use of all available resources to first mitigate the problem in progress, then recover whatever can be recovered and use it to build on new data in place of or to replace the destroyed data.

Exercises

1. What are the differences between online social networks and online communities?
2. Discuss the social problems of online social networks.
3. An ecosystem is a localized group of interdependent organisms together with the environment that they inhabit and depend on. How do you relate this to online social networks?
4. Discuss privacy issues that apply in your online social ecosystem.
5. Discuss five modern online crimes.
6. Discuss strategies that can be used to effectively eliminate (if possible) online social network crimes?
7. If you were to write a framework to prevent cybercrimes from online social networks and indeed from all online spaces, what would be in it?
8. Is cryptography all we need to secure computer network and protect information?
9. Why is cryptography failing to protect digital systems and information? What do we need to do?

References

1. Fox R (2000) News track: age and sex. Commun ACM 43(9):9
2. Bylaws for internet corporation for assigned names and numbers. ICANN, April 8, 2005. www.icann.org/general/bylaws.htm
3. Evolving the high performance computing and communications initiative to support the nation's information infrastructure—executive summary. www.nap.edu/readingroom/books/hpcc/exec.html
4. Kizza JM (1999) Ethical and social issues in the information age. Springer, London
5. News & events: web surpasses one billion documents. Inktomi. www.inktomi.com/news/press/billion.html
6. Kizza JM (2011) Computer network security and cyberethics, 3rd edn. McFarland Publishers, Jefferson
7. Communication from the Commission to the Council and the European Parliament. Commission of the European Communities (Com2000), p 202. www.europa.eu.int/eur-lex/en/com/cnc/2000/com2000_0202en01.pdf
8. Information age haves and have-nots. www.library.wustl.edu/~listmgr/devel-1/august1998/00058.html
9. Schroeder S Facebook facing $138,000 fine for holding deleted user data. http://mashable.com/2011/10/21/facebook-deleted-data-fine/
10. Wikipedia: cyberstalking. http://en.wikipedia.org/wiki/Cyberstalking
11. http://www.bullyingstatistics.org/content/cyber-bullying-statistics.html
12. BBC News. http://news.bbc.co.uk/2/hi/technology/7056264.stm
13. Young K (1998) Internet addiction: the emergence of a new clinical disorder. Cyberpsychol Behav 1(3):237–244
14. Neville Misquittaa in "Psychiatry and Society in Pune". http://blog.pathfinderclinic.com/2011/02/social-networking-psychological-effects.html
15. Walsh M Court backs student on Facebook page criticizing teacher. NewsWeek. http://blogs.edweek.org/edweek/school_law/2010/02/court_backs_student_on_faceboo.html
16. Kizza JM, Network C (2005) Security. Springer, New York
17. Newman D, Whitaker A Penetration testing and network defense: performing host reconnaissance. http://www.ciscopress.com/articles/article.asp?p=469623&seqNum=1&rl=1
18. Tittel Ed Understanding security policies. http://www.informit.com/articles/article.asp?p=25041&rl=1
19. Hayes B Conducting a security audit: an introductory overview. http://www.ecurityfocus.com/infocus/1697
20. Unavoidable ethical questions about social networking. Mekkula Center for Applied Ethics, Santa, Clara University. http://www.scu.edu/ethics/publications/submitted/social-networking.html