Chapter I
Cybercafé Systems Security

Lawan Ahmed Mohammed
King Fahd University of Petroleum and Minerals, Saudi Arabia

ABSTRACT

This chapter introduces the vulnerability and security issues associated with the use and operations of Internet cafés or cybercafés by demonstrating different methods of launching different attacks especially when using commercial Internet cafés in a way that renders the system or other systems inoperable. It discusses the challenges facing those operating and managing Internet cafes, governments, parents, and even educators to ensure proper preventive measures, guidelines, and laws needed to protect the system against breaches, misuses, and abuses. It also argues that defense mechanism against breaches should be dynamic and strong enough due to the increasing number of new freely available cracking tools and harmful Web sites. In addition, virus, worms, Trojan horse, adware, malware, and spyware are spreading beyond imagination. Further, the chapter discusses different defense mechanisms.

INTRODUCTION

Throughout the world, information and communications technologies (ICT) are generating a new industrial revolution already as significant and far-reaching as those of the past. It is a revolution based on information, itself the expression of human knowledge. Technological progress now enables us to process, store, retrieve, and communicate information in whatever form it may take, unconstrained by distance, time, and volume (Bangemann et al., 1994). In many countries, computer networks are used to control, manage, and operate system services. Transportation, banking, power system, radio and television, gas, water, health services, telecommunication, and

the like are highly automated and computerized. Therefore, the Internet is not really about computers only; it is about people, communication, and sharing information and knowledge as well as overcoming physical boundaries. Further, the focus in computing environment today is moving away from the desktop and becoming diffused into our surroundings. The ubiquitous paradigm foresees devices capable of communication and computation embedded in every aspect of our lives and throughout our environment. In such pervasive computing environments, these requirements will increase both the complexity of information infrastructures and the networks which support them. Some of these reports can be found in (Kagal, Tim, & Anupam, 2001). These systems, in addition to defense, government, and education form part of a society's critical information infrastructure. While the Internet offers access to tremendous educational, leisure, and social opportunities. On the negative side, as more and more computers are connected to the Internet, the networks are becoming more vulnerable making it easy for an intruder to attack systems in many ways. As such, the rate of computer and cyber crimes has accelerated beyond imagination, with continual increases in incidents of cracking, hacking, viruses, worms, and bacteria having been reported in recent years. Therefore, businesses, companies, and organizations both private and public must be mindful of cyber crimes and safeguard their systems.

Throughout the past decade, governments or policy makers, businesses and industries, parents, and educational sectors, especially in the more technologically advanced countries, have tried to address the problem of cyber crimes from different perspectives. Moreover, there are clearly dangers and risks to younger generations in what is largely a new, unregulated medium especially when using public cybercafés or Internet cafés. It is important at this juncture to define the term cybercafé. As defined in Summers (2005), *cybercafé or Internet café is a public place where you can pay to use the Internet and buy drinks etc*. Other common usages include Net telephony, college and employment applications, stock trading, Web site maintenance, in addition, of course, to the e-mail, chat, and computer gaming. In this chapter, we discuss some security threats associated with the design and usage of cybercafés and discuss some counter measures.

PROBLEMS WITH CYBERCAFÉ SECURITY

Security on the Internet is, by its very nature, highly interdependent. Each Internet system's exposure to attack depends on the state of the security of the rest of the systems attached to the global Internet. Because of the advances in attack technology, a single attacker can relatively easily employ a large number of distributed systems to launch devastating attacks against a single victim. From a business point of view, a single virus or other forms of cyber attack could cause extended downtime, which would have a negative impact on the whole business. Moreover, tools such as firewalls, virus scanners, and intrusion detection systems are rapidly maturing, but rapid technology advances, a plethora of non-secure products, and the growing complexity of corporate networks diminish their effectiveness.

The security of cybercafé systems can be discussed based on two security dimensions:

1. **System security:** The technical innovations and managerial procedures applied to the hardware and software to protect the privacy of the records of the organization and its customers
2. **Network security:** To protect the networking system as a whole and sustain its capability to provide connectivity between communicating entities (Yang, Lu, & Zhang, 2006).