CURRENT SECURITY TRENDS AND ASSESSMENT OF CYBER THREATS

by

BIJITESHWAR RUDRA AAYUSH

B.E in Information Technology, Bharati Vidyapeeth University, 2009

A Report Submitted in Partial Fulfillment
of the Requirements for the Degree of

Masters of Computer Science

In the Graduate Academic Unit of Computer Science

Supervisor: Rodney H. Cooper, MMath, Computer Science

Examining Board: Wei Song, Ph.D., Computer Science, Chair
Natalia Stakhanova, Ph.D., Computer Science

This report is accepted by the
Dean of Graduate Studies

THE UNIVERSITY OF NEW BRUNSWICK

January 2015

©Bijiteshwar Rudra Aayush, 2015
Abstract

Continuous functioning of critical infrastructure is one of the foundations for the socio economic activities and development of a country. Owing to the continuous development in technologies, computers, other computing services, software and cyber space are used for interconnection, information processing and communication. The development in technology and the use of cyber space have created new threats and vulnerabilities which could pose at least as significant a threat as a physical attack. Lately cyber criminals and terrorists are using their skills to exploit cyber space and they are committing severe crimes.

The objectives of this Masters report are to explain the role of cyber space and computing technologies on critical infrastructure and highlight several cyber threats and countermeasures. This report also highlights the need of secure software development and explains how an average programmer can contribute in securing cyber space and what effect that can have on national infrastructure.
Acknowledgements

First and foremost, I would like to express my sincere appreciation to my supervisor, Prof. Rodney H. Cooper, for his guidance, encouragement, assistance, patience, and motivation in completing this report.

I also wish to express deep and sincere feelings to my family for their encouragement throughout this long endeavor of completing this report.
# Table of Contents

Abstract ........................................................................................................................................ ii

Acknowledgements ..................................................................................................................... iii

List of Figures .................................................................................................................................viii

1.0 Introduction ............................................................................................................................. 1

1.1 Objective .................................................................................................................................. 2

1.2 Overview of the Report ............................................................................................................ 3

2.0 Introduction to Critical Infrastructure and Cybercrime ......................................................... 5

2.1 Infrastructure ......................................................................................................................... 5

2.2 Critical Infrastructure ............................................................................................................. 6

2.3 Cybercrime ............................................................................................................................. 7

2.3.1 Offences against the confidentiality, integrity and availability of computer data and systems ................................................................................................................. 10

2.3.1.1 Illegal Access ............................................................................................................. 11

2.3.1.2 Data Espionage ........................................................................................................ 11

2.3.1.3 Data Interference ..................................................................................................... 12

2.3.1.4 System Interference ............................................................................................... 12

2.3.1.5 Cyber Terrorism ...................................................................................................... 13

2.3.2.1 Computer related fraud ......................................................................................... 15

2.3.2.2 Computer related forgery ..................................................................................... 16
2.3.2.3 Identity theft ................................................................. 17

2.3.3 Content-related offences .................................................. 17

2.3.3.1 Child pornography ....................................................... 17

2.3.3. Libel and false information ............................................. 19

2.3.3.4 Other forms of illegal contents .................................... 20

2.3.4 Copyright-related offences ............................................. 20

2.3.4.1 Piracy ............................................................................ 21

3.0 Cyber Security ........................................................................... 23

3.1 Background ........................................................................... 23

3.1.1 Information security ....................................................... 24

3.1.2 Mobile Security ............................................................. 27

3.1.3 Network Security ........................................................... 30

3.2 Countermeasures .................................................................. 34

3.3 Critical Infrastructure Protection (CIP) ............................... 39

3.3.1 Critical Infrastructure Protection Life Cycle ....................... 41

4.0 Coding Standards, Guidelines and Best Practices ................ 44

4.1 Background ........................................................................... 44

4.2 Types of Standards ............................................................. 47

4.3 Secure Coding ....................................................................... 48

4.4 Coding Techniques ............................................................. 49
5.4.6 Weaknesses in authentication and authorization ............................................. 72
5.4.7 Use of hard-coded credentials ...................................................................... 73
5.4.8 Invalidated redirects and forwards ............................................................... 73

6.0 How Programmers Can Write Secure Code ....................................................... 75

6.1 Background .......................................................................................................... 75
6.2 Programmer’s Resources ..................................................................................... 76
6.2.1 Security oriented courses and specialized degrees ......................................... 76
6.2.6 Security audits .................................................................................................. 82

7.0 Conclusion and Future Work .............................................................................. 84

7.1 Conclusion ............................................................................................................ 84
7.2 Future Work ......................................................................................................... 86

Bibliography ............................................................................................................. 88

Curriculum Vitae
List of Figures

Figure 1 Critical Infrastructure Protection Event Cycle .................................................41
Chapter 1

Introduction

For the continuous functioning of the socio-economic activities of a nation, certain sectors that make up the national infrastructure of a nation must work reliably and effectively. Sometimes a few sectors play a critical role for a nation and its people and these sectors are called critical infrastructure. Situations like the unavailability and disruption of the critical infrastructure can significantly impact the life of modern society.

Whether it is infrastructure or critical infrastructure, there are a few common denominators such as computers, networks and cyber space acting as bridges, connecting everything together. In the later part of the 20th century, computer and software applications were introduced in critical and non-critical work areas, which not only simplified tasks but also eliminated human mistakes. Since that time computer and computing components are preferred in most areas. Whether it is a public or a private enterprise, without computers and cyber space, it is hard to imagine the continuous functioning of scheduled tasks. The introduction of computers and cyber space eliminated flaws and human errors; however, the popularity of this approach also introduced cyber threats including hacking and cyber terrorism.

Cyber space is still under exploration and is getting denser with information. Securing cyber space is getting more important. Researchers around the world have tried to study and understand reasons for cyber vulnerabilities and threats.
Owing to the modernization, application development plays a critical role in critical infrastructure. However hackers and cyber criminals try to find vulnerabilities in the developed applications and exploit the application users. These exploitations can be significantly reduced by producing secure code. Programmers need to identify how badly developed code can have a significant impact on its users. They need to understand various secure coding standards developed by organizations, such as OWASP and CWE, and they should integrate their recommendations and best practices in the application development process to move one step toward secure application development.

1.1 Objective

The main objective of this Master’s report is to explain infrastructure and what makes it critical in modern society. It will also explain the importance of cyber space and how it acts as the backbone in the functioning of the critical infrastructure of a country. This report will highlight cybercrimes and discuss major types of vulnerabilities and flaws in software systems.

Furthermore, this report will also explain and access current security threats to critical infrastructure and cyber space. It will explain various categories of cybercrime and explain its impact on modern society.

This report will explain how improvement in the area of the software development process can have a significant impact in securing web space, and result in a more secure infrastructure. It will also highlight the need of various programming
standards, guidelines and best programming practices in the secure software development process.

1.2 Overview of the Report

Chapter 2 of the report will provide a background on the infrastructure and critical infrastructure of a nation and highlight the nine sectors of critical infrastructure as defined by the Canadian government. A detailed description and categorization of cybercrime will also be explained.

In chapter 3 of this report, cyber security will be presented. This chapter will discuss the impact of cyber security on information, mobile and network security and will also focus on various countermeasures that are currently applied and others that are being considered for implementation to achieve security. Moreover this chapter will explain the need for critical infrastructure protection along with the critical infrastructure protection life cycle.

Chapter 4 of this report will concentrate on various coding standards, techniques, guidelines and best practices that can be used by programmers in order to produce error free code.

In chapter 5, secure coding and best programming practices will be explained. This chapter will also explain the role of secure coding and secure application development in modern society. It will focus on a few organizations which publish security standards for software professionals, and it will also highlight a few major security flaws and weaknesses recognized by these organizations.
Chapter 6 of this report will highlight various resources for programmers. These resources are proactive and reactive measures that can be integrated while programming to help programmers produce secure and violation free code.

Chapter 7 of this report will provide some conclusions including some options for future work.
Chapter 2

Introduction to Critical Infrastructure and Cybercrime

This chapter provides basic information on critical infrastructure and cybercrimes. The Patriot Act of the USA defines Critical Infrastructure as [1]:

“Systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.”

Section 2.1 describes Infrastructure; Section 2.2 explains Critical Infrastructure and section 2.3 describes Cybercrime.

2.1 Infrastructure

Infrastructure refers to the available facilities and services required for the proper functioning of a country. In general it can also be defined as services required to sustain and enhance the life standard of general society. Infrastructure includes, but is not limited to water pipelines, telecommunications, food, finance and energy. On the basis of importance and functionality, infrastructures have been divided into hard and soft. Hard infrastructure represents physical means and structures that serve the country such as transportation, communication infrastructure and energy transfer whereas soft infrastructure represents the social frameworks that are required to preserve the cultural, social and economic health of a country [2].
2.2 Critical Infrastructure

An infrastructure can be called a Critical infrastructure (CI) or Critical National Infrastructure (CNI) when any disruption in its functioning can significantly affect the day-to-day life of society in general and hence can result in political and security chaos. Services offered by critical infrastructure are extremely important in the proper functioning of an economy and government. The Federal Emergency Management Agency (FEMA) defines critical infrastructure as "personnel, physical assets, and communication (cyber) systems that must be intact and operational 24x7x365 in order to ensure survivability, continuity of operations, and mission success, or in other words, the essential people, equipment, and systems needed to deter or mitigate the catastrophic results of disasters. [3]."

Critical infrastructure can also be defined by the immediate dependence and complex dependencies. The immediate dependencies, for example, can be between energy and water or electricity and transportation or even telecommunication and transportation. Any disruptions of these dependencies can have negative effects. In case of complex dependencies, a functionality can be dependent upon another and that dependency might not be apparent. Hence knowingly or unknowingly, damage to one component can have a direct effect on another [4].

Depending upon the national strategy, every nation might categorize critical infrastructure differently. Canadian national strategy divides critical infrastructure into 10 sectors. These sectors are:
a. Energy and utilities
b. Finance
c. Food
d. Transportation
e. Government
f. Information and communication technology
g. Health
h. Water
i. Safety
j. Manufacturing

Apart from critical infrastructures, the national infrastructure of a country also defines key assets which are key resources of extreme national importance. According to the Department of Homeland Security, key assets can be symbolic targets whose destruction would not have a vital effect on the nation, but can create local disaster, and damage a nation’s morale. Key assets refer to museums, monuments and heritage sites which emphasize national pride, prestige and reputation. Key assets also include facilities that deserve special protection because of their value to a local community and facilities that represent national economic power and technological advancement [98].

2.3 Cybercrime

The word cybercrime reminds one of those 1990’s movies involving teenagers who used to live in basements and who tried to hack into government systems just for the fun of it. But, in reality, in those days, the world was still fighting mostly physical crime,
and cybercrime had little impact on society. But now with the change in the nature of technology along with easy access to facilities, the term cybercrime means a great deal more and has a bigger domain and more impact. The world is now experiencing a change in the nature of crime.

One of the main reasons for this transition is the rapid expansion of the internet, especially with the absence of a regulatory authority. A decade or more ago, when the internet was a growing facility cybercrime was mainly a military issue, but now it is a major concern of all society. With no central authority and control over its usage and protection there exist serious gaps in security which can be exploited. Initially cybercrime was considered to be unorganized crime with limited impact such as unauthorized accesses and file transfers, but today those small crimes have turned into profit making organized businesses, and have evolved into an organized business structure.

Cybercrime is a term used for any kind of crime in which either computer, mobile devices or networks are objects of the crime or they are used to commit a crime. Hacking, or spamming are examples of computing devices being the targets, whereas child pornography and cyber frauds are examples of cases where computing devices are used to carry out crimes.

Cybercrime can be committed by one individual or a group of individuals, and it can target personal computers, servers and mobile devices. Cybercrime is now one of the most popular ways of creating stress and chaos in a society. In this technological era, every facility and service is dependent on computer systems and uses virtual space for information transactions. This gives more choices for rich targets to the cyber criminals.
Cybercrime is emerging as a challenge for national and economic security, and owing to its evolving nature, many public and private sector organizations are at constant risk. According to the Department of Homeland Security, cyber-attacks are getting more and more popular among criminals, and the number of cybercrimes is increasing in comparison to any other medium of crime [23]. The reason behind this popularity is that these attacks require neither a big investment nor do they need many experts to execute an attack. Sometimes a cybercrime needs only an internet connection or someone with the specific set of skills and knowledge to attack the system.

Modern enterprises rely on technology and that technology has become the backbone for the whole gambit of modern infrastructure. Most organizations share services with each other, for example, the use of IT services in the transportation sector or the use of energy in water and manufacturing sectors. Sharing of services has not only created a dependency of one resource on another, but this interconnection has also created opportunities for fraud and theft. As a matter of fact depending upon the type of an organization, the exploitation of gaps created by these dependencies can have a significant impact. For example, attacks on the banking sector can have a significant impact because a nation’s economy depends on its banking sector. Any security malfunction can be externally and internally exploited. Offenders on both ends can exploit any weakness they can find in the system.

Along with the birth of new crimes, the internet has also accelerated the rate of traditional crimes, providing criminals with a new way for easy communication and for carrying out transactions with the additional advantage of “absolute anonymity”. For
example, according to reports published by the United Nations [5], criminals using payment gateways for money transactions cannot be tracked easily.

There are several types of cybercrimes which are hidden and go unreported owing to reasons such as loss of reputation, revenue, lack of experience, unavailability of resources, ignorance, and so on. According to the council of Europe: convention on cybercrime, cybercrime offences are normally classified into four major categories [100] which are:

a. Offences against the confidentiality, integrity and availability of computer data and systems
b. Computer-related offences
c. Content-related offences
d. Copyright-related offences

2.3.1 Offences against the confidentiality, integrity and availability of computer data and systems

Any (or all) offence which compromises the confidentiality, integrity and availability of digital information falls into this category of cybercrime. This category normally includes attacks directed towards a computer system and/or the data. According to the council of Europe [101], illegal access, data espionage, data interference, system interference and cyber terrorism are types of this category.
2.3.1.1 Illegal Access

This term refers to the group of crimes which are committed in order to gain access to a computer system and information without the knowledge and/or consent of the authentic user of the system. Hacking is often considered to be an example of Illegal access.

a. **Hacking**: Hacking normally refers to any unlawful access to a computer system, illegal access to some public or private network and critical information theft using faulty hardware and infected software. Hackers exploit poorly designed applications with the help of software, viruses, Trojan horses or malware. Breaking the password of computer systems and password protected websites and using the information obtained for financial and personal gain or launching attacks of higher intensity are some of the most common examples of hacking and cracking [100].

2.3.1.2 Data Espionage

Data espionage refers to stealing information of highest value of a country or even a user such as military and trade secrets, business secrets and other high value data from computer systems often with the use of the internet. With the expense of very little time and money, a mass audience can be reached through the internet and therefore sensitive information stored on computer systems connected via the internet are often targeted by cyber criminals. Cyber criminals use social engineering techniques such as phishing and
intrusion techniques such as port scanning [104] to acquire access to sensitive information.

2.3.1.3 Data Interference

Data interference refers to attacks that compromise the integrity and availability of computer data. Computer data can be private or public information either stored or processed by a computer component. Today cyber criminals and offenders target computer data for several reasons such as financial or personal gain. The Council of Europe Convention on Cyber-Crime signifies data interference crime as intentional damage, alteration and deletion of computer data, and electronic components, or any electronic message including the introduction and transmission of a virus.

2.3.1.4 System Interference

According to Lennon Yao - Chung Chang [102], “system interference refers to serious hindering of a computer’s ability to function by intentionally inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.”

System interference also refers to any physical attack targeted by/ on a computer system and its hardware which can significantly impact the day-to-day business. For example, industries such as banks and telecommunication companies are providing 24 hours availability and accessibility for its users, hence any physical damage to the computer and hardware components which are involved in this process can result in significant loss for the business and the users.
2.3.1.5 Cyber Terrorism

Over the years there have been several definitions of cyber terrorism. One of the definitions offered by the FBI’s special agent Mark Pollitt is that "Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub national groups or clandestine agents [9]." In short, Cyber terrorism is the use of technology by terrorist organizations to execute terrorist activities. These activities include and are not limited to hacking into government networks, disrupting military communications, disrupting critical infrastructure and so on. Developed countries like The United States of America, Russia and Canada or developing countries such as India and Pakistan, are all at war with these terrorists and facing the threats of cyber terrorism.

Terrorist organizations now have educated masterminds who are fully aware of the ways a system can be penetrated. These masterminds execute cyber-attacks using malware such as computer viruses and Trojan Horses and worms and they illegally access files and information which are extremely sensitive for a nation. Generally these attacks are responsible for causing extreme physical or economic damage which leads to nationwide loss and extreme chaos. These cyber terrorists can hack into secret file systems of a government and sell the secrets to the highest bidder and they can also hack into the military facilities of a country to steal important information about a nation’s current strength and strategic planning. These terrorists can also cripple a nation’s economy by hacking into financial facilities such as banks and national stock exchanges.
Several reasons why cyber terrorism is turning out to be such an attractive option for the terrorists [10] are as follows:

**Maximum Damage and Unlimited Number of Targets**: Generally sectors of any major facility are connected through a private network. If the terrorists can get access to any single section, they can shut down the entire facility and depending upon the criticality of that facility, the unavailability of its functioning can even jeopardize the national security. If a traditional way is considered such as a missile launch, the damage and its effect will be limited, whereas the damage caused by a cybercrime using an internet connection can have a long lasting effect. These terrorists could target the critical infrastructure such as energy or the telecommunication sector which can cripple the entire system.

**Cheaper Method**: It is considered to be a comparatively cheaper method than other traditional methods. In the case of cyber terrorism, a terrorist might need just a computer and the internet connection instead of spending millions on weapons such as missiles and explosives. For example, they can create a virus or a Trojan Horse and use an internet connection to infect applications and servers even if the targets are geographically apart. Instead of using weapons to target one location at a time, cyber terrorists can infect a number of targets such as networks of governments and public utilities at the same time and create chaos around the globe [10].

**No Need to be Physically Present**: With the help of the internet, terrorists attack a country even though they are halfway around the world from the target. Compared to conventional attacks such as detonating a bomb using a detonator, the internet involves no danger of being a suspect or even danger to one’s life during the attack [22].
2.3.2 Computer Related Offences

Computer related offences relates to crimes that are committed through the use of a computer system. This category includes offences such as computer related fraud, computer related forgery and identity theft [100].

2.3.2.1 Computer related fraud

Computer related fraud is a crime that makes larger profits by committing a number of smaller offences. They are targeted towards computers and data processing systems for fraudulent purposes. Generally in this case offenders make a larger financial profit by targeting a number of victims. Since the loss seems to be smaller, these frauds either go unnoticed or victims of these crimes normally don’t spend too much time in investigating these losses. Nigeria advance fee fraud is one such example [103]. Two of the most common computer frauds are online auction fraud and advance fee fraud.

a. **Online auction fraud**: Online auction is one of the many ways through which sellers can reach to a massive audience and buyers can access special goods irrespective of the geographical distance from the seller. With more and more acceptance of ecommerce services, the online auction is considered to be one of the fastest growing businesses in the current marketplace. However the popularity of the online auction is also turning into tempting targets for cyber frauds. In this case, the victim bids for a product and receives notification that he/ she have won the bidding. Later victim makes the payment but never receives the merchandise. Cyber criminals are taking advantage of the absence
of physical face to face contact between a buyer and seller and due to which distinction between a genuine user and a fraud is getting much more complicated. This type of fraud includes sale of non-existent goods, advance payment for the goods and delivery upon payment with no intention of paying, using legitimate user names and passwords to buy and sell goods fraudulently [100].

b. **Advance fee fraud:** Advance fee fraud is a well-known fraud where victims, generally internet users are tricked into paying a small sum of money in return for receiving a substantial benefit. In this case offenders send photographs, documents, files and several legal documents to a victim to prove their legitimacy. These offenders generally impersonate as higher government officials and attorneys and convince a victim that the victim has won a prize or a lottery or some other financial prize and which can only be received by the victim if the victim agrees to pay a small fee in advance. By paying the fee, not only the victim risks losing the paid fee amount, but also risk losing more in several different ways such as credit card fraud or fraud courier charges requests and bank processing charges [100].

### 2.3.2.2 Computer related forgery

Computer related forgery relates to cybercrimes that use computer systems for unauthorized creation, alteration or any kind of manipulation of digital data such as digital images, files, documents and even non-existent documents originating from credible institutes.
2.3.2.3 Identity theft

Identity theft involves stealing one’s private information, bank account numbers, credit card numbers, social security or insurance numbers, license numbers and also the illegal access to personal computers and smart phones. This type of crime existed before the internet, however the usage of the internet has taken it to a whole new level. One of the ways this type of crime is carried out is with the use of spyware [20]. Once spyware is installed onto a computer or a smart phone, it collects private information and uploads the data to some kind of storage device used by the thieves. This data can be used for monetary purposes or worse for committing other frauds in the name of the victim.

2.3.3 Content-related offences

This category of cybercrime covers content which is considered illegal and is normally targeted towards individuals, races, religions and organizations. Following are the categories of content-related offences.

2.3.3.1 Child pornography

Pornography involving the use of children as sex objects is called child pornography. Normally it includes a recorded act of child sexual abuse or even a direct sexual assault. This problem has been in society for a long time, but with the popularity of cameras, and the internet, child pornography has become an immediate area of attention for authorities. According to a report published by the United Nations [5], “most of child pornography transmitted today is in electronic form and the pornography industry uses the internet to transmit it. According to reports published by the Council of
Europe, a computer system and the internet together is used for the purpose of distributing, transmitting, procuring and storing child pornography [101]. Before the internet, the primary distribution channel for child pornography was through regular shipping or physical delivery. However post internet, the whole situation changed dramatically. Internet based data exchange and decreasing prices of technical equipment made the production and distribution service not even easy, cheap and less time consuming but it also provided an extra layer of anonymity to remain undetectable from authorities [101, 100]. There has been other research on how these crimes are committed and how electronic porn videos are distributed. The abusers use fake commercial and non-commercial websites along with peer-peer transfers and password protected forums. Over the years, authorities have tried several ways to locate the databases of these images and videos and they were surprised by the number of pictures and videos they recovered. Combating Online Pedophile Networks in Europe (COPINE) at University College York in Ireland collected images from various known and unknown databases and discovered over half a million images [5].

Authorities from all over the world have tried to contain the situation as must as possible. According to reports published by United Nations [5], internet not only provides a safe distribution system to the offenders, but it also provides a virtual payment system to its users in cases such as commercial child pornography and therefore tracking the money flow sometimes becomes impossible for the authorities.
2.3.3. Libel and false information

The Internet is considered to be the cheapest and sometimes easiest method to announce and broadcast information. In most cases general users come across several known and unknown facts on websites, posts, tweets, messages and blogs. However the information available is not always correct or even true. The Internet can and is also used to spread misinformation as easily as information. The Internet also provides enough anonymity to its users that anyone can post any false and defamatory fact or information about a person, group, race, community, organization and even a country without any kind of permission and verification. Sometimes social networking websites which are extremely popular among users of all ages are used to spread malicious content. The unavailability of regulations and authority verification have often offered offenders the opportunity to spread facts and information which are sometimes false and sometimes too sensitive for the general public, for example, intimate and sexually compromised photo shopped images, secret business information, disclosure of military secrets, etc. Similarly, sometimes false and misleading information can be a vital reason for defamation. Through the internet, a massive crowd can be easily reached without spending too much time and money and often offenders take advantage of this fact. Several cases have been registered where cyber criminals use false emails to send misleading information about public figures and organizations which significantly impacts the reputation and image of the targets [100].
2.3.3.4 Other forms of illegal contents

Digitization has motivated today’s society in such ways that now the internet is considered to one of the primary methods to learn and educate. Whether it is a course on programming or basic calculation, business or biology, the internet can help anyone learn anything. However depending upon the user, the same internet can be dangerous as well. For example, the internet not only has information and courses on chemical engineering, it can also be used to teach someone how to build explosives, similarly not only does it instruct the user on how to make a business transaction, it can also be used to learn how to hack someone’s bank account. The popularity and availability of the internet has made the learning process easy and less time consuming and therefore increase in the likelihood of events such as cyber-attacks, cyber espionage and hacking in compared to the era before the internet where information transaction was not only difficult but also time consuming.

2.3.4 Copyright-related offences

Copyright relates to exclusive legal right of owners and originators on anything they create. It assures the ownership over anything that has been created and gives the right to print, publish and film to its owner or anyone else that has been authorized by the owner. Until the later part of the 20th century, most of the data transfer was dependent on mediums such as physical books, audio and video tapes. Medium of data transfer was limited and hence smaller chance for illegal production of available data. However in the generation of tablets and smartphones, digital data is not only proving to be important necessity in terms of storage and availability but it is also proving to be an extremely
popular choice among users of all ages. Whether it is a word document, an audio clip, a software or even a movie, digital data has been accepted as the current trend. However, the need of accessibility and availability of digital data has also given birth to several copyright issues; one of those issues is known as piracy. Piracy includes offences such as software piracy and music or movie piracy.

2.3.4.1 Piracy

The illegal and unauthorized copying, reproduction and distribution of copyright materials is called piracy. Earlier, offenders used to manufacture illegal duplicates of copyright materials and cater it to the market of users who cannot afford authentic products due to the high prices for example, in 1990s video compact disks were considered a popular choice in the movie piracy business [102]. However the generation of digitization and the popularity of the internet among have accelerated this crime. Today, the internet is being used as a main source for illegal distribution of products for example, expensive software, films, songs, etc. Industries all around the world are facing serious financial problems due to piracy. Especially in a case of software piracy, where a software firm invests millions of dollars to create new software, illegal copies are created from licensed copies and later on distributed with the help of the internet. Internet users easily download the pirated version via torrent and other sharing sites at very less or sometimes no price at all. Apart from software industry, piracy has significant impact in games and film production industries as well where producers spend million and billion dollars to create a new game or produce a new movie and cyber offenders illegally copy the product and distribute it via the internet as soon as it is released to the market. In
some cases, pirated contents are sold under the pretense of genuine product at the same
price of authentic product to the users who are not familiar with the product [102].
Chapter 3

Cyber Security

This chapter provides basic information about cyber security. According to Isaac Ben-Israel, cyber security advisor to the Israeli prime minister [11],

If you want to hit a country severely you hit its water and power supplies. Cyber technology can do that without shooting a single bullet.

Section 3.1 presents background on cyber security, Section 3.2 describes countermeasures being taken by authorities in terms of securing cyber space, and Section 3.3 explains the critical infrastructure protection and critical infrastructure life cycle.

3.1 Background

Cyber space is considered to be an important amenity for modern life and today cyber space is not limited to business transactions or government institutions; it has extended itself into the lives of the common citizens of a country. Currently, email money transfer is preferred to going to the bank and waiting in a queue and online shopping is chosen over going to the store for shopping. With this much dependence on the cyber world, cyberspace needs to be protected from present and emerging threats. Currently securing cyber space is a very big challenge for any nation.

Cyber security continues to be a field of continuous research. Three of its most important domains are Information security, Mobile device security and Network security.
3.1.1 Information security

According to the Committee on National security Systems (CCNS) [88], information security is the process of protecting information and its critical elements. This process also includes the protection of systems and hardware that are directly and indirectly responsible for processing, storing and transmitting the information. The scope of information security is not just limited to securing the information; it also includes information security management, computer, data and network security [89]. Owing to the popularity of the internet, public and or private sectors are extensive users of this channel of communication. Since most of the information flows over this channel, security of this channel should be the priority of any country. A piece of information can be a coded military message or a presidential directive and cyber criminals and terrorists attempt to break through security measures so that the information can be stolen and used for some other purpose. Sometimes a piece of information can be extremely critical to an organization and its safe transmission can be a tough task for the organization. Lately more and more data is stored on computers and other digital devices and transmitted using computers and smart phones. Hence, the issue with information loss not only affects every government or business, but it can also affect every person.

The organization for Economic Co-operation and Development proposed the following nine principals for security of information systems [12]: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. Information security depends on following core principles [27]:
1. **Authentication:** The process of validating a user is called authentication. In general, user provided information such as user ID or user name is compared against user personal information such as passwords. However in some cases, depending upon the criticality of the system and information, other user personal identifications such as government issued identification numbers, palm prints and retina scans can be requested for authentication purposes. Upon successful validation, the user is given access to the requested information [89].

2. **Integrity:** Information integrity means maintaining the consistency, accuracy and reliability of information. Precautionary measures should be selected so that no change can be introduced by the attackers.

3. **Availability:** This refers to the availability of information under any circumstance. Information must be available and a user must be able to access it when needed. No disruption in power or a hardware and software failure during the time of any other physical or virtual attack, should interrupt accessibility.

4. **Confidentiality:** Confidentiality ensures access of information to authorized users yet at the same time preventing sensitive information reaching to the hands of wrong people. For example, information such as credit card numbers, bank account numbers and secret files should be accessed by the user who is either the owner of information or is someone who is authorized by the owner to access the information.

These structures are interrelated, and for proper functioning of information assurance and transactions, they all need to work together. If a message is sent over a channel, the most important thing is to ensure whether the message is genuine or not, i.e.,
the sending party and the receiving party are in fact who they are claiming to be. A message’s authenticity is an extremely important feature; an important message can be sent by someone pretending to be someone else, and a message can be stolen and a new altered message can be received by the receiving party. Similarly, in terms of information integrity, the accuracy, consistency and reliability of the content of a message needs to be unaltered over its entire life cycle. Criminals and terrorists target different messages floating in cyber space, and they can make changes to the content of some important but insecure messages. And finally, the availability of the message is an important concern. A message needs to be available at all times in spite of any hardware or software malfunction. In fact, a message should be available even after any cyber-attacks are targeted to steal critical messages.

3.1.1.1 Classification of information

In electronic space all kinds of information is being transmitted from one party to another. Since the threat of information leakage is always there, information needs to be secured. But before that, every piece of information needs to be classified, which depends on the organizations and their security classification scheme.

The government of the United Kingdom classifies the information in following categories [90]:

a. Official

b. Secret

c. Top Secret
The classification of information for the Canadian government is as follows [91]:

a. Classified

1. Top Secret
2. Secret
3. Confidential

b. Designated

1. Protected A (low-sensitive)
2. Protected B (particularly-sensitive)
3. Protected C (extremely-sensitive)

Sometimes information classification is done on the basis of the risk tolerance level of the organization. It depends on the information, its nature, and how valuable and vulnerable the information is in terms of the organization, and the client.

3.1.2 Mobile Security

Along with computers, cyber space is also shared with mobile technology, in fact, with the continuous development in the field of smart phones and tablets; it has been a popular choice over conventional desktop computers and laptops. Today mobile devices have also become a primary concern for security professionals all around the world. More and more users are using smart phones and tablets for almost all day-to-day activities. Not only in the outside world but also within an organization these devices are proving to be extremely critical. With the development of small yet powerful applications, the communication industry has reached new limits. There are applications for mobile
banking, online dating, messaging and so on, but these transmit extremely sensitive user information. These profound changes in communication technology, which are making the life of a user very comfortable, are also becoming the source of risk for a user as well as an organization.

The attacks on a mobile device are generally carried out via a means of communication, such as messaging (SMS, MMS) or mobile networks especially wireless networks, Bluetooth, infrared etc. There are several other directed and undirected attacks on a user, which include, GPS tracking, blocking access to facilities on mobile devices, the recording of conversations etc.

Military professionals, scientists or common citizens can have extremely sensitive as well as regular information on their devices, such as military secrets, new research, personal bank account numbers, personal messages etc. Once cyber criminals get their hands on any such information, they can attempt several things. A few of the recent incidents include:

a. Criminals can program the phone to record and send a copy of all future communications to them, which can be used against the victim

b. The attacker can stop messages from being received.

c. The mobile simcard can be copied and therefore it can be used to make phone calls to paid services or unrestricted numbers in the name of the victim.

d. Information stolen from the device can be used in identity theft.

e. Attackers copy and remove all the personal files on the victim’s device. These files may contain important images, videos, address books, etc.
The attacks on mobile devices can be physical, but at the same time they can be targeted toward other domains of a mobile device.

3.1.2.1 Attacks targeted at software applications

Every mobile device is equipped with an operating system along with software such as web browsers, etc. With the mobility advantage, many people prefer mobile devices over any laptop or desktop and use it for purposes such as storing information which might be critical to the user such as bank account and credit card numbers, browsing emails and the internet via web browsers [26], downloading applications and games etc. These mobile devices not only have advantages, but they also pose huge and significant threat for their users. For example, use of the internet is not entirely safe because most of the web browsers either have extensions or they require extra widgets such as plug-ins. These widgets are downloaded from some external source, possibly some unsafe source, which can be a major threat in the mobile industry. Also the downloaded applications are not always secure. Some of the applications pretend to do something else, but in truth they are malware and spyware whose purpose is to collect sensitive information from the phone and send it to the hacker. These malicious applications not only make the phone vulnerable, but with the information stolen, it can make the user vulnerable as well. Apart from these threats, mobile devices also present some significant physical threats. For example, the devices can be stolen and if there are no protection systems on the devices, the stored information can be used to carry out other frauds and criminal activities.
Mobile devices such as mobile phones and tablets have become extremely popular among all generations, but all of these devices use wireless technologies, and it is not always possible to have a safe network connection. Owing to this fact, cyber criminals are now targeting networks, especially wireless networks.

3.1.3 Network Security

Whether it is a computer or a server or a mobile phone, everything is connected via a network; hence, networks can be summarized as the most important area of concentration for security. A network can have different meanings in terms of different situations. For example, there can be a home network connecting mobile devices, computers, laptops, etc. Similarly, there can be a big corporate network of an organization which might have laptops, computers, mobile devices, servers, virtual networks, etc. There can also be big government networks for a province or even a nation. Cyber criminals always try to get unauthorized access to these networks so they can use the resources, get access to devices on the network, get privileged access and steal information. There have also been several complaints regarding these cybercriminals gaining access to networks and launching denial of service attacks and modifying configurations without the knowledge of the network administrator or network users. In some cases, when public networks are involved, the victims are not only administrators or government officers but most of the victims are part of the general population. In 2012, the Indian Railways website was hacked by cyber criminals, which not only caused trouble for government employees, but it also had a disastrous effect on the general population. Railway employees lost connection with the servers, the railway
reservation web portal denied access to employees all around the country and railways passengers and travelers were not able to buy tickets due to the disruption in the online and offline reservation systems.

With the popularity of wireless networks, securing a network has become extremely difficult. Wireless connections are based on wireless nodes and access points and hackers tend to exploit any vulnerability they can find without a direct connection to these nodes. Wireless communication has a very large domain; it includes personal computers, laptops, tablets, mobile phones and so on. With many critical devices in any network, hackers try to gain access to the networks and can target any or all of the devices.

The attacks on networks have been categorized as [25]:

a. **Active attack**: An attack which is executed with the help of viruses, worms or other types of malware to get unauthorized access to secured systems. These attacks target secure data transmissions, and the attacker tries to steal and/or modify important information. Some of the active attacks are:

1. **Denial of service**: The primary goal of a denial of service attack is to deny the access to a particular resource to its intended users. This interruption of resource can be temporary or it can be for a longer period. Generally these attacks are directed toward websites, web applications, servers and web services. These attacks are executed by either increasing the traffic load on a channel hence flooding a network, disrupting connections between servers and terminals, causing physical damage to the resources,
modifying configurations and consuming resources. These attacks can have a significant impact on an organization. The size of the impact can vary depending upon the size of the organization.

2. **Spoofing**: A spoofing attack is when an attacker or a group of attackers impersonates another device in order to launch attack on network hosts, gain unauthorized access to either steal critical information or modify the current settings for access control. There are different types and methods of spoofing for example IP address spoofing, DNS server spoofing, and ARP spoofing [92, 99].

3. **Attack on physical facilities**: An attack that causes disruption due to any physical damage to the equipment. Transmission of data highly depends on network connection. To establish a network, sensors and nodes are sometimes placed in unattended and hostile outside environments. Attackers can intentionally damage the nodes permanently or they can even extract some device related secrets, modify the configuration of sensors and infect the nodes [93].

4. **Buffer overflow**: Modifying a file by overwriting the allocated memory sector. Generally attackers find some poorly developed applications and they exploit them by overwriting values of certain registers, and base and instruction pointers. After overwriting the values, the application tends to generate errors and exceptions. Buffer overflow can be executed using stack overflow or heap overflow.
b. **Passive attacks:** In passive attacks, the attacker targets the information via intercepting the traffic. Rather than breaking in to a system or stealing/ modifying the information, in this case the attacker keeps listening to the information which is being transmitted such as passwords and other sensitive information and sometimes these attackers also publish this unauthorized information. Possibly this sensitive information is also used to execute other types of attacks. And since in this attack the information is never altered, it is really very hard to detect and therefore the attacker can keep stealing important information for a long time.

Some passive attacks are:

1. **Release of sensitive content:** In the past decade, there have been cyber-attacks where subversive organizations steal sensitive information from private and public organizations so that it can be either distributed or published on general forums. Some of the information may be extremely sensitive such as a company’s accounts or a government’s agendas and so on [96, 97].

2. **Traffic analysis:** In case of traffic analysis, messages which are being transmitted, are closely examined and intercepted. No message is modified, however the content of messages either secure or insecure is read. Passive attacks are very commonly used by terrorists and militants to steal military and political secrets [94, 95, 97].
3.2 Countermeasures

Securing cyber space is not only the responsibility of cyber security professionals; as a matter of fact, knowingly or unknowingly computers and internet users contribute to some kind of cybercrime. After gaining illegal access to computers, servers and public and/ or private networks, cyber criminals can launch a cyber-attack. Hence, a secure cyber world can only be imagined when everyone is ready to contribute.

Over time, researchers and cyber security professionals from all over the world have faced problems and disruptions all owing to cyber criminals and they have proposed several policies, standards, and countermeasures to contribute to securing cyber space.

However depending upon the situation, the responsibility of securing the web space varies from regular user to application programmer to security professional. In general, securing the information in transition is the most important goal in cyber space, and securing this transmission, without any interruption or alteration is extremely important.

Information can be secured using several proposed techniques and policies. According to a report published by IEEE [13], some of the techniques and policies for information security are as follows:

1. Proper identification of the roles and responsibilities of every user. Any user in an organization should be well aware of the domains and there should not be any access to the user outside the domain of the assigned work.
2. In case of any public or private organization, a security team should develop security policies for the organization. The team should also be responsible for making sure that the policies and guidelines are being followed.

3. Change management is part of every organization, but a requested change should be authorized and approved. The management needs to make sure that the requested change is not only safe but that it also will not interrupt the day-to-day operations.

4. Information security is a shared responsibility; therefore all users and employees should be provided proper training or some awareness program regarding information security.

5. The management of an organization or even a user should always be aware of current security threats and vulnerabilities and similarly implement appropriate countermeasures.

6. Updates and revisions should be installed as soon as they are released, so that in case of a new possible vulnerability, the current system can be protected.

7. Continuous security audits are extremely important for an organization. These audits discover security gaps and any impacts on the applications owing to those gaps. These audits highlight the sections that need revisions and maintenance.

8. A contingency plan should always be in place, which should explain recovery strategies for the system users and for an organization in case of any intrusion, information leakage, or any kind of interruption.

Like other network systems, mobile communication needs to be safe as well. With all the advancement in technologies, mobile communication has become the backbone of
communication networks. The following are some of the best practices for secure communication.

1. **Application download centers:** Today smartphones are extremely popular and one of the reasons for this is the availability of mobile applications. Applications are of every type, including banking applications, some popular game apps, email apps or even an internal organization application. Mobile users download all these applications where they are required, but not all sources of these applications are secure. There can be some hidden malware and worms to infect the mobile. To keep the communication secure, users should evaluate the source of the application. They should read the reviews and experiences of other users before downloading applications.

2. **Trusted web links:** Mobile phones, especially smartphones, are heavily used for the internet access. It is probably the most popular device among the younger generation and working professionals. Therefore users should be aware of the risk of opening untrusted web links. Hackers infect mobile phones using web browsers and infected pop ups, hence the users should pay attention to the websites. In particular working professionals using an organization’s mobile phones should be alert for any redirected websites and only continue if they are aware of the new portal. No user should fill in private information on the websites they are not familiar with and if any information is requested, they should inspect the web address.

3. **Password protection system:** Mobile phones should also be protected from any physical intrusion. An intrusion can happen internally or externally; for example,
some friend or some employee may try to steal some information for personal or professional reasons, or a stolen mobile phone without password protection can be used to retrieve some personal information. Therefore a user should always keep password protection on any kind of mobile device.

4. **Firmware updates:** As soon as a new update arrives, a user should always update to the latest version. Latest versions not only update applications but they also update the security features of a device.

5. **Security application:** Users should install security applications such as antiviruses on mobile devices. With the popularity of mobile phones, hackers and intruders are swarming the web space with viruses and malware. A security application can notify the user whether the device might be infected if a site is visited or if an application is installed.

6. **Resource consumption:** A device user should monitor usage of resources on a mobile device. For example, unexpected usage of battery and memory is a sign of malware infection. Mobile users should periodically check the running applications and inspect their usage along with the battery consumption.

Network protection is another fundamental need for secure communication. Whether it is a wired network or a wireless network, security is the highest priority. For a secure network, various countermeasures need to be in place, such as:

1. **Physical safety:** The computers and other devices on a network should reside on a safe environment free from any kind of physical damage. Especially in the case of some application critical system, the systems running the applications should
be kept separate and safe with maximum restriction on access. There should not be any issues such as electric failure.

The safety of the location of a critical system is also necessary. The network equipment should be kept safe from general users so that there cannot be any tampering with the equipment. The facility should be inaccessible to anyone who is not authorized to work on network devices. Facilities should have identity recognition systems for users, and access control should be installed so that unauthorized sections cannot be accessed.

Physical protection should also be in place for some natural calamities and disasters. A few parameters should be in place to keep things running even in the case of any natural disaster.

2. **Technical safety**: Securing a network technically is most important. Over time, several countermeasures have been proposed and established.

   a. Network access control should filter out the authorization and access should be provided accordingly. A user in a network, should be identified and the access to resources on a network should be provided accordingly. Especially in the case of any private or organizational network, no outside user should have access and even the internal users should be provided access according to their needs.

   b. Networks should be regularly inspected and scanned for any kind of intrusion or viruses and malware. In case of an infection, remedies should be applied on the network as well as on any device that was connected via the network.

   c. Firewalls and anti-virus software should be in place for filtering the contents.
d. USB keys and disks should not be allowed to be used on a private network. An internal or external attack can easily be carried out via removable media.

e. Back-ups and logs should be recorded so that in the case of an attack, the intruder can be identified and the system can be rolled back to a safe state.

3.3 Critical Infrastructure Protection (CIP)

As discussed in section 2.2, Critical Infrastructure are those facilities which are vital for the proper functioning of a nation, including those required for national security, public health and safety and the economy, and whose destruction or disruption can have a very debilitating effect. Since the continued functioning of critical infrastructure is so significant for a country, it has also become a very tempting target for hackers, cyber criminals, and cyber-terrorists. Therefore critical infrastructure protection has gained paramount importance all over the world. Countries are establishing policies and security measures along with new laws to protect their critical infrastructure.

After the 9/11 attacks, countries recognized the threats that cyber criminals and terrorists posed to national security. Countries started installing security measures and taking precautions against any threats they might face. The Bush administration formed the Department of Homeland Security (DHS) in the United States of America. The initial job of DHS was to identify, prioritize and protect the critical infrastructure of the nation. DHS analyzed all the infrastructure and realized that cyberspace is the common factor along with several interdependencies. Based on their research, they recognized that securing a critical infrastructure is also a subset of securing cyberspace. The DHS identified five priorities to secure Critical Infrastructure and Cyberspace [23]:

39 | P a g e
1. A National Cyberspace Security Response System
2. A National Cyberspace Security Threat and Vulnerability Reduction Program
3. A National Cyberspace Security Awareness and Training Program
4. Securing Governments’ Cyberspace
5. National Security and International Cyberspace Security Cooperation

These five priorities define the complete cyberspace protection system of the United States of America. Similar to the Department of Homeland Security, Canada’s Royal Canadian Mounted Police (RCMP) has established a Critical Infrastructure Intelligence Team. The responsibility of this team is to oversee any possible physical and virtual threats to the Canadian infrastructure. Protecting critical infrastructure also involves the Canadian Cyber Incident Response Centre (CCIRC) which has been assigned new responsibilities, such as monitoring threats, incident management and information sharing.

According to a paper published by the Government of Canada [15], there are 9 key elements of a Critical Infrastructure protection strategy.

1. Guiding principles
2. Risk Management
3. Information sharing
4. Inventory of Critical Infrastructure assets
5. Threats and warnings
6. Critical Infrastructure interdependencies
7. Governance mechanism
8. Research and development

9. International cooperation

The ultimate goal of these key elements is to strengthen the resiliency of the critical infrastructure of Canada.

The Indian government has established an Inter Departmental Information Security Task Force (ISTF), which examines any national threat, oversees the protection of critical infrastructure, develops information security and cyberspace security awareness and provides training programs. Apart from this, several initiatives have been taken by the government including conducting R&D activities, establishing security policies, performing security audits, and forming a security response team.

3.3.1 Critical Infrastructure Protection Life Cycle

According to reports prepared by SATRC Working Group on Policy and Regulations [14] and CEPS Task Force Report [16], the critical infrastructure protection framework life cycle is a six phase process:

![CIP Event Cycle](image)

Source: US Department of Defense.

**Figure 1 Critical Infrastructure Protection Event Cycle [14]**
1. **Analysis and assessment**: This is the initial and foundation phase of the protection life cycle. This step is used for identification of all key assets which are critical to the successful accomplishment of any mission. Once the analysis is complete, the critical assets are assessed and key vulnerabilities are identified. After recognizing the crucial assets, all the other dependencies and characteristics along with the impact of unavailability of the infrastructure are also analyzed.

2. **Remediation**: This phase includes all the countermeasures that need to be in place to guard against a future attack that could compromise a critical asset. In this phase, all the known cyber and physical attacks along with some possible future attacks that can interrupt the normal operation of critical infrastructure are considered and remedies are prepared. The aim of this phase is to make the critical infrastructure reliable and available even in a time of national crisis.

3. **Indications and warnings**: This phase is used to monitor and assess all the processes necessary for mission accomplishment involving critical infrastructure and to determine if any incident needs special attention. In this phase, a scheduled infrastructure event is examined on the basis of any operational or strategic level input. The source of these inputs can be asset owners or any regional assets such as government agencies, intelligence agencies, law and enforcement agencies, or any key private sector actors. On the basis of these inputs, all the operational changes are inspected and the data owners are notified of any risk or possible threat.
4. **Mitigation**: This phase involves any/all of the actions that can be taken before or during an event in response to warnings and incidents, so that the impact during the unavailability of a critical infrastructure can be minimized.

5. **Incident response**: This phase describes all the plans and actions that should be executed in response to an incident such as a physical or cyber-attack on a critical infrastructure.

6. **Reconstitution**: This final phase is comprised of all the actions that can be taken once a critical infrastructure is destroyed or made physically or virtually unavailable. This phase describes plans and procedures needed to restore the facilities and their functioning.
Chapter 4

Coding Standards, Guidelines and Best Practices

This chapter will discuss coding standards and guidelines in general. It will also highlight some guidelines and best programming practices released by several organizations around the world.

4.1 Background

The demand for new applications in almost every field and industry has promoted a rapid growth in the field of software development. Various commercial and non-commercial applications are being developed every day to achieve the goals of clients. Over the last two decades, organizations of every size have considered software development as a highly productive field.

Software development companies assess clients’ needs and specifications, and develop applications accordingly. But along with applications used by general society, there are some sensitive applications such as those for the military or for use in the research and development sector. These sensitive applications require special emphasis on the reliability and security of information contained therein.

Therefore, organizations all around the globe have developed programming styles, coding standards, and guidelines for software professionals to follow. In general, these standards ensure that programmers produce uniform code. These standards and guidelines are not only useful for the application developer or programmer, but are also
used as a framework for software development by software architects, managers, analysts, etc. They guide application programmers in writing good quality, violation-free clean code, and programmers and developers are expected to follow these sets of instructions.

However, coding styles are not always consistent; different organizations use different platforms and languages, and the style of coding varies depending upon the language an organization is using. These standards allow programmers to code in a common and uniform way, so that if necessary, a programmer even in a remote location, can easily make changes to the source code without extensive recoding and risk of failure. Especially in the case of open source software, programmers use the source code and change it according to their needs; hence, uniformity in code generation is important.

But that is not the only reason why one should follow coding standards. If the coding standards are followed properly, the following should be the result:

1. Reviewing the code should be much easier. Since the programmers should develop high quality, properly written and maintained code, it should be easy for them to understand.

2. Working on an application developed using a fairly new language should not be that difficult for programmers who are not familiar with the language.

3. Working in a consistent environment should improve code reliability. A programmer during a change management process should easily be able to discuss any change with colleagues, if they are following the same standards.
4. There should be no discrepancies in a team of programmers. If a consistent standard is being followed on a project, there should not be any conflict in programming styles.

5. Following a standard from the initial phase of the software development process requires a thorough understanding of the working of the software. These standards can highlight some basic yet important changes in the architecture of the software in the initial stage of development so that the organization will not have to spend more in terms of time and money.

Following coding standards is extremely productive for an organization. It can prove to be advantageous in terms of writing as well as maintaining software. Sometimes an application might have been written more than a decade ago, and the author might not be working on the same application any more or may have left the organization. In these cases, maintenance can be an overhead for any new developer and conformance to standards can be extremely advantageous.

Furthermore, following coding standards means high quality code with fewer or no bugs. Change in the functionality/operation of a program is very common in the software industry. However, any change can introduce bugs or conflicts in the working of the application. Following coding standards means fewer conflicts after any requested change. If the code is developed by following the standards and guidelines, it is much easier to test. Software organizations stress existing code standards not only to save on expenses but also to accelerate the software development process so that they can cater to business needs as soon as possible.
However, some developers do not adhere to such standards and tools, mostly because they may result in too much extra work owing to the errors and warnings about non-compliance with rules.

### 4.2 Types of Standards

During the application development process, a project can and should adhere to the following standards [17]:

1. **Language specific standards**: Different projects use different development languages. Even in one organization, there can be several projects using different languages. Sometimes even the style of a programmer working on a project can significantly vary from that of other programmers working on the same project. To resolve these conflicts, language specific standards should be used jointly with general and project standards. Language specific standards direct the programmers to use a unique set of standards throughout the life cycle of the project. Even in the case of development using different languages and styles, following the standards is always recommended.

2. **General standards**: General standards highlight how a programmer should write the code. Regardless of the platform and language of the project, these standards should be followed by the developer. General coding standards highly recommended following internal documentations and the practices explained in it.

3. **Project standards**: These standards are set according to business needs. In general, these standards should work in accordance with general and language-specific standards. Project standards can be developed by any organization which
is undertaking a project; i.e., these organizations can be public or they can be private. These standards are based on the nature of the project, and they can be changed accordingly. Sometimes, depending upon the similarity of projects, the standards are also adopted from other organizations. However, in some cases there can be some conflict between project standards and language or general standards, and in that case, project standards will have priority.

4.3 Secure Coding

The demand of computer software and applications, and the number of exploitations and attacks on those software applications have developed the need of secure applications which can guard itself from defects, bugs, or any other software attacks. To prevent the system from vulnerabilities, security measurements should be placed throughout the software development life cycle.

According to researchers and professionals, one of the root causes for so many exploitations and vulnerabilities of software is insecure coding. Language experts, skilled software developers and security researchers and professionals around the world have suggested secure coding and developed secure coding standards that can be followed by application developers to prevent the bugs, defects which can make the software vulnerable to any outside or inside attacks [55, 56].

Secure coding plays a major role in the development of a secure software. Secure coding is the process of writing programs by following uniform set of rules defined for the project by the organization instead of following no standards or the standards which
are familiar by the programmer. Secure coding is important for all software irrespective of the language used for development or the domain where the software will be used.

As explained in section 4.2, several coding standards such as language specific standards or general standards have been developed over the years and which are being followed by software developers. However professionals around the world also prefer to use secure coding along with these standards. Software development standards help programmers write clean and structured application and adding security to the application along with those standards reduces the possibility of bugs and security threats which can make the software application vulnerable to possible attacks. As explained earlier, the standards are irrespective of development language or framework and they are set according to the business rules, therefore including security constrains enhances the capability of software in terms of a secure environment for information transaction.

4.4 Coding Techniques

Based upon the coding standards, coding techniques consists of various processes used in the software development life cycle. They incorporate many different phases that contribute to quality code development which includes basic programming, scripting, and any query languages. Coding techniques also contribute to developing a new or updating an earlier version of coding standards.

Generally they are classified into three categories [18, 19]:

1. Naming conventions
2. Comments
3. Format

4.4.1 Naming conventions

Proper naming in the software development process is probably the most important aspect of coding. A name of a variable, procedure, array, or even a class explains what it is being used for. The appropriate naming convention is also very helpful in understanding the logical flow of the code. Most projects are developed by a team; hence, every team member has a specific duty. For example, a team member might be assigned to write a piece of code for some functionality. In these cases, a proper naming convention would be extremely helpful for other team members when they add that functionality in the final code. For example, AddNewMember() would be much more explanatory than writing AddNew(). Not having a suitable name can produce unnecessary complexity in the code. It is not always important to select a short name; longer names can be used in the program as long as they explain their functionality to a reader and are not too wordy.

According to Microsoft [18], programmers should follow these guiding principles:

a. Programmers should avoid ambiguous names. The names of the variables and functions should be explanatory enough to interpret their functionality. For example, to display the total values, ShowTotalValues() can be used instead of TotalValues().

b. The name of the class should not be used inside a class or property.
c. Any function used for arithmetic computation should include appropriate abbreviations in the name of the function. For example Add, Mul, Sub, Avg should be included in the name of the function.

d. Mixed case formatting should be used during the naming process. Mixed case highlights proper differentiation especially when the name is a little longer.

e. Names which are generally used as Boolean variables should be avoided, such as true, false, and flag.

f. A single alphabetic character, should be used only for a short lived functionality, such as i and j, which are two of the most used letters; generally they are used as counters in a loop. If the scope of these variables is wider than expected, they should be replaced by a meaningful name.

g. Constants should always be uppercase. In the case of a longer name, underscores should be used.

h. If a column inside a table is created, it should not contain the name of the table.

For example, for a table named Employee, Salary should be the name of the column instead of EmployeeSalary.

i. If a function is supposed to return a value, the function should be named accordingly.

j. If the code uses an external source, such as a file or folder saved on the disk, the folder should be named accordingly. For example, if the folder is used for images, it should be named images or pictures or something explanatory.

k. A name should not be used again for some other purpose. Even if the name is used in some other section, it leaves the readers and other programmers in a state
of ambiguity and they might have to spend more time in understanding the difference.

4.4.2 Comments

Comments are explanations that a developer writes on the source code at the time of developing some new functionality, control or class. Developers are expected to write these comments in parallel with the development. These comments are not necessarily of any use to the author but for a different developer, they can be very helpful. Typically authors are expected to write a little about the working of the newly developed section along with the date and details on variables.

The following are a few of the techniques which are widely used:

a. With the start of development, authors should provide details about the new section. These details can be but are not limited to the purpose of the function, expected results, any assumptions, etc.

b. After any update or modification in the code, the date should also be updated.

c. Comment the code using a uniform style throughout the application.

d. Comments should be written for important sections of the application. Commenting is a very good practice, but code should be commented only when it needs to be. Commenting on every line increases complexity unnecessarily and sometimes creates ambiguity for other programmers.

e. These comments should be explanatory and should be written in a professional way so that every user can understand the functionality of the section.
f. Code should be commented at the time of writing only. Apart from special sections, programmers should only comment during bug fixes and important updates.

4.4.3 Format

The logical and visible organization of the code is called formatting. If the source code is written and formatted in a consistent way, it not only looks clean and unambiguous but it can be extremely helpful in understanding the logical flow of the program.

A few of the most important conventions which should always be followed are:

a. Open and curly braces should be vertically aligned.

b. As soon as new code is introduced, indentation should be checked and the code should be formatted accordingly.

c. Indentation should always be consistent. The number of spaces between lines of code should always be uniform. Proper indenting makes it easier to read and understand the flow of the code. Special attention should be paid to a loop or condition.

d. Naming conventions, especially naming a variable with mixed case alphabets, should be followed to ensure that similar constructs have a similar appearance.

e. SQL queries should be on separate lines. Reviewing code is easier if the name of the table and the clause are properly differentiated.
f. In SQL uppercase should only be used for keywords; mixed case on the other hand should be used for database elements.

g. While writing a new section, especially a condition or a method, programmers should make sure that the method or the condition is responsible for limited functionality, preferably a single one. This way the code will be organized and understandable for other programmers.

4.5 Guidelines

While both standards and guidelines are widely used and have proved to be extremely helpful, there is a very fine line differentiating these two. Where coding standards are expected to be followed, these guidelines are not mandatory at all. Organizations, depending upon the project, set the standards that should be followed by their programmers, however guidelines are not mandatory, although programmers are strongly encouraged to integrate them in their code while developing.

The following are a few of the guidelines programmers should incorporate in their code:

a. Developers should follow proper spacing practices for better readability and understandability, especially between two operators. Depending upon the language, difference in spacing can mean a completely different operation.

b. Every line should have only one statement. In the case of expressions, multiple assignments and nested statements, unless it is necessary, should be limited to one per line.

c. Variables should always be followed with their type.
d. Programmers should always provide comments, especially for any new section they developed or are about to develop. These comments prove to be very helpful for other programmers working on the same project, and in some cases for the author of the code as well. Programmers can write details about the functionality and operation followed by date and time of creation. Comments also differentiate between lines of code which provides better readability and helps in organization of the code.

e. Programmers should try to write simple and neat code instead of long and complex code. Simple code is good for other programmers and reviewers to understand and at the same, changes can be made easily if needed.

f. A subroutine or function should not be too large in terms of lines of code. An excessively large section can create complexity in the logical flow of the program.

An organization, whether it is a multinational software firm with many employees, resources and projects, or a small startup business with few employees and projects, always encounters situations such as violations, errors, new changes and updates in the software, and the author of the code may not be there to fix any issues. Hence this change management process can take a lot of time for other programmers and at the same time it can be extremely expensive in terms of resources and disruption in the business.

The lack of standards in the development process or failure to comply with the standards has become a very important subject of discussion around the globe. These standards not only ensure the organization and especially the software developers produce quality code, but also provide a proper set of guidelines to prevent any violations.
Several organizations have published their coding standards, not only because they help in maintaining the code quality, but also because they prove to be very helpful in the testing phase of the application. However, these practices are not always followed by the developers and programmers. The reason behind this is that programmers have time constraints and are too busy writing the code or they do not realize the importance of these standards, or sometimes they are not aware of the standards at all.

Over the years, a few alternate options have also been proposed that can be followed to maintain the standards. They are as follows:

1. **Training**: Before programmers start writing the code, proper training should be provided on the relevant standards and guidelines. This training should also explain why it is necessary to follow the standards along with the requirements of the project and expectations of the client.

2. **Audits and Code reviews**: Frequent audits and code reviews should take place. These audits and reviews should also inform the programmers whether or not they are following the organizational and project standards. Along with other changes in the code quality, they should also direct the programmers if any section of the code needs some special attention.

3. **Analysis tools**: Depending upon the language and standards, several analysis tools have been developed. The main goal of these tools is to help programmers write good quality code. These tools check the code as per the needs of the programmer, and provide a detailed report on all the violations and errors. Today, this option is considered over the other two because not only do these tools
provide instant results to the author of the code, but also by using them, the programmers can remove most violations without waiting for the audits and review results.

These tools are not just good for the programmers but they are proving to be very profitable for the software firms as well. By the use of these tools, programmers remove most of the conflicts and violations and therefore it takes a lot less time for the audits and code reviews. Also programmers produce better code without the constant guidance of senior programmers and managers.

Quality code production is a very important concern and software professionals are trying to implement as many precautionary measures as they can. New strategies and techniques which can help firms produce violation-free software are constantly under development. However the most important foundation is still the knowledge and participation of programmers who will have to understand how these standards, guidelines and best practices can help them achieve their goals.
In this chapter secure coding will be discussed in detail. Section 5.1 will define secure coding. Section 5.2 will highlight the role of secure coding in modern society, especially to protect the critical infrastructure of a country. Section 5.3 will present background on some organizations and secure coding standards prepared by those organizations, and Section 5.4 will highlight some major security vulnerabilities.

5.1 Secure Coding

Secure coding is a very broad term and an understanding of the term "secure" is necessary. Including commercial and non-commercial software, every year thousands of applications are developed. Billions of lines of code are produced by numerous software developers around the world.

These applications fall into the following categories [21]:

1. System software: The software is developed for making a device operational and controlling the functionality of a device. A few common examples of system software are operating systems, device drivers and graphical user interfaces.

2. Application software: This type of software is used to perform a specific operation. This software has limited functionality and its working is limited to particular sections. They are also dependent on the device and the system
software. A few of the examples include office applications, anti-viruses, entertainment applications and weather applications.

System and application software are used in public and private sectors and can be extremely critical to their user bases. They are used in financial and medical sectors as well in sectors of critical infrastructure such as transportation, energy, etc.

With the adoption of computers and software by almost every industry, information security has become a challenging task. The areas of operation are wide and the range of the applications is wider; therefore, the threats and risks of information leakage are extensive. Hackers, cyber criminals and terrorists penetrate software using Trojan Horses, viruses, worms and other malware. In fact, the mediums of these attacks are not limited, and every now and then, hackers find a new way to get illegal access into these applications; they steal information and cause disruption in their day-to-day operation. The effects of these attacks can be extremely severe depending upon the criticality of the application and its area of operation.

Chapter 4 discussed a few of the basic standards programmers should follow to improve the quality of the code. However, following the code standards makes programs more understandable and code more readable. The impact of code quality is limited to the logical flow of the code. But even after following these code quality standards, the software can still be compromised.

According to professionals in the software and security industry, one of the main reasons these many threats and vulnerabilities occur is sloppy and poorly written code
The need for software is escalating in every field; therefore the demand for software developers is increasing exponentially. But the code that is produced by these developers does not always meet high standards. The software development not only lacks quality, i.e., code project and organization standards, but also fails to meet security standards. Organizations need to consider security from the very beginning of the software development life cycle. Improving the quality of software requires various considerations, and one way to achieve this is through adopting secure coding practices.

Secure coding is the practice of writing programs that are free from any bugs, defects or any other software flaws so that the software can guard itself in case of any malicious activity such as hacking and any illegal access. Secure coding helps in achieving the safety of critical information from any kind of cyber theft or attack. Malicious users such as hackers and crackers keep looking for vulnerabilities in applications and use those vulnerabilities to commit crimes such as breach and bypass computer and the internet security, gain illegal access to networks, destroy files, steal critical information such as credit card number or personal information of a victim and infect application servers. Many of these vulnerabilities result from software programming errors which are found and exploited by the hackers and crackers [83].

In fact these attackers are also skilled and experienced programmers. In some cases, these programmers offer their services to several organizations where they review and access the code. Once they review the code, “ethical hackers” highlight the sections which need security controls. However in other cases, these expert programmers take advantage of the flaws in the code and cause considerable damage. Depending upon the
nature of the software and its area of operation, programming flaws can be responsible for revealing corporate, personal and private information, enabling terrorist activities, and allowing cyber theft [24].

5.2 Role of Secure coding in modern society

As explained earlier, software applications are used in almost every field in modern society. One of the most important consumers of software is national infrastructure. Unlike private organizations, public organizations are dedicated to serving the citizens of a country. Therefore, any incident involving a government facility can have a direct effect on its people. The impact of the threat elevates when it has the ability to affect any national infrastructure, especially any national critical infrastructure. The entire security community is threatened by the number of insecure applications used by countries, governments and their citizens.

As mentioned earlier, professionals around the world agree that insecure coding is one of the most important reasons for so many incidents of hacking and cracking. Professionals do believe that not every attack or security incident happens due to poorly written code; however it is an important factor. Failure of software owing to poor programming, can have a catastrophic effect, and combining it with an improper architecture can have major consequences. If programmers do not develop quality applications, hackers and cyber criminals can take advantage of poorly written code. Over the years, cyber criminals have hacked several sectors of government facilities in various different countries. The attackers stole information, caused disruption in the operations of infrastructure, and created panic situations in the country.
Secure coding is very important for every application, and when the application is responsible for proper functioning of a government, secure coding becomes a much broader term. Software applications are used in every sector of critical infrastructure, i.e. they are used in transport, health, energy and utilities, finance, manufacturing and so on. These sectors use applications such as web applications, control applications, databases, etc. These applications contain regular to critical data such as addresses, social insurance numbers and bank account numbers. Several countries have faced numerous hacking attempts on their critical facilities over the last decade. These incidents not only directly affected the society, but they also resulted in disruption of proper functioning of infrastructure and hence cause a huge loss of lives and money.

When it comes to cyber-attacks, most are directed towards the organizations which are in a business that involves a nation’s critical infrastructure. Security professionals believe that if the programmers had followed some security parameters and written the code accordingly, most of these attacks could have been avoided [53, 54]. Following the secure code standards and practices will minimize the risk of any threat.

5.3 Organizations and Popular Coding Standards

Over the years, the terms application security and software security, have been used continuously. Several applications have been hacked and attackers have stolen secret and critical data. Although software engineers and security professionals have made a lot of changes, they have not yet met industry and user expectations because programming practices have changed little [55]. The reason for sloppy coding has always been a debatable topic among software professionals. To eliminate the threat of
exploitation, several secure coding standards have been published by different organizations.

The following are a few of the organizations and international security standards that can be referred by software professionals:

1. Computer Emergency Response Team (CERT)
2. Open Web Application Security Project (OWASP)
3. MITRE
4. Payment Card Industry (PCI) Security Standards
5. Microsoft Secure Coding Guidelines

5.3.1 Computer Emergency Response Team (CERT)

CERT refers to the group of software experts which handle computer security related incidents. CERT is a Carnegie Mellon University (CMU) initiative, which originally focused on security issues including malware, worms and computer viruses. This team recognized that when it comes to security, programming was one of the areas which needed immediate attention. They provided several standards and sets of coding practices for a number of languages, so that the programmers can effectively integrate these practices while developing applications. Also these standards could be used as the framework for organizational standards [28].

In the later years of the 20th century, CERT practices were directed towards languages such as C and C++, because not only were these languages a popular choice for coding, but they were also used in developing critical infrastructure applications. With
the development of new technologies, new programming languages have forced this
group to develop new sets of practices which should be compatible with available
programming languages [28]. CERT is still not recognized as an international standard,
but its standards are based on standard language versions which are defined by
organizations such as ISO/IEC. Along with other standard groups, CERT is continuously
working on various guiding principles and practices.

5.3.2 Open Web Application Security Project (OWASP)

This organization focuses on improving software quality by educating developers
about various threats, risks and vulnerabilities. OWASP is a free project, which means
OWSAP users can be an organization or even a developer; everyone has access to
OWASP guidelines. OWASP enables programmers to develop, update and maintain
more secure applications.

OWASP has never been a part of any particular technology or a particular
language. This project is considered to be a secure application initiative. Organizations
use OWASP to produce secure code and to improve software security through preparing
organizational guidelines, building tools, and compiling checklists and other internal
documents [29]. Based on the vulnerabilities and threats, every year since 2004, OWASP
has identified the top 10 most critical security flaws for web applications [30].

5.3.3 MITRE

MITRE is a non-for-profit, organization which works in partnership with
government and operates federal sponsored research and development centers established
to addresses critical national issues [84]. Every year since 2009, MITRE prepares a list also called as MITRE’s CWE which is a formal list of the top 25 most dangerous software vulnerabilities and weaknesses in collaboration with the SANS Institute [33] and security professionals from the USA and Europe [31]. This list of vulnerabilities highlights the most widespread and critical errors which can result in major software flaws. These vulnerabilities are easy to find and exploit and they can be used to steal data and even disrupt the working of software.

Similar to OWASP, this list is used mainly for educating programmers as well as the consumers and making them aware of the security flaws and their impact on an application. It identifies the critical flaws and weaknesses of software and explains how a developer can avoid the common mistakes. After the development phase, senior management can follow the CWE guidelines to test the software and identify any security flaw. MITRE works closely with the government facilities in the United States of America, especially with US Department of Homeland Security [32]. It collaborates with the US Department of Homeland Security to provide detailed description of errors and security measures organizations can follow to avoid and mitigate the security flaws [31].

5.3.4 Payment Card Industry (PCI) Security Standards

PCI standards [34] are specific to organizations involved in the transaction, storage and any other processing of card data, especially credit and debit cards by banks, independent sales organizations (ISOs), online shopping carts, retail merchants, etc. [35].
These security standards are developed by the Payment Card Security Standards Council [34, 36]. This standard organization is a collaborative initiative of American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa [36] and their purpose is to develop, publish and revise industry standards for all developers and security professionals who work in the card industry.

5.3.5 Microsoft Secure Coding Guidelines

Microsoft software tools are among the most popular and highly accepted tools around the world and are used by millions of developers to produce applications. These technologies are used by various public and private organizations to develop software to cater to the needs of different sectors. Since Microsoft technologies are so popular, there have been several security incidents such as hacking and cracking. As a result Microsoft researched and prepared *Microsoft Secure Coding Guidelines* [37] and *Microsoft .NET Framework Secure Coding Guidelines* [38]. These guidelines are specific to Microsoft technologies where the application code can reuse the infrastructure; however in situations of additional security, developers can enhance the security functionality using new and customized methods [37]. These standards not only guide the developers to write secure code but also guide system administrators on security critical resources.

All of the above organizational standards are used all around the world to write, update and maintain secure code; however they are not restricted to developers only. These standards are also heavily used in testing applications for security vulnerabilities. These guidelines and practices are also used by analysts and upper level management.
5.4 Security Vulnerability and Flaws

Poor programming practices and non-compliance with security standards often lead to development of software with vulnerabilities and security flaws. Based on the organizational standards, a few of the major security flaws and weaknesses are as follows [39, 40]:

1. Injection flaws
2. Insecure direct object references
3. Security misconfiguration
4. Sensitive data exposure
5. Missing function level access control
6. Weaknesses in authentication, authorization, or cryptographic practices
7. Use of hard-coded credentials
8. Invalidated redirects and forwards

5.4.1 Injection attacks

Injection attacks represent the family of attacks that corrupt the normal execution of web applications by injecting invalid, malicious and untrusted code into a program so that they can read, delete and modify data on a website. Two of the major injection attacks are SQL injection and cross-site scripting. [41]
5.4.1.1 SQL Injection

Injection of corrupted SQL queries via input data in an application is called the SQL injection attack. Through this attack, malicious SQL queries are inserted via the client side in an application to get access to secure communication channels. Once the attackers get access, they can not only read data from a database but also delete and modify stored data [42]. Via a successful SQL injection attack, the attacker also can sometimes get administrator privileges and therefore all the rights for different operations on a database.

This type of attack can be easily prevented by applying input validation techniques. Via input validation, a user credentials can be compared and authenticated against business and previously defined set of rules for length and syntax. Developers should be cautious while writing and using stored procedures. Mistake such as concatenating arguments in a stored procedure is highly injectable. Unused stored procedures should be removed from the application. Also the access to database should be granted to specific users [85].

5.4.1.2 Cross-Site Scripting (XSS)

Cross-site scripting is a type of injection attack which is considered to be one of the most dangerous attacks on web applications because it allows the attacker to steal sensitive user data [43]. This attack is executed by injecting malicious scripts into trusted web applications. The attacker embeds malicious scripts in a browser and sends it to the victim, and since the victim’s browser has no way to ensure whether to trust the script or
not, the browser will execute the script [42]. The corrupted scripts can hijack user sessions and can access any previously saved sensitive information such as passwords and bank account numbers.

To prevent this type of attack, the programmer needs to determine input path for the website through which it accepts user input. Executable code should never be accepted as an input value. Programmers should implement filters along the pathway that should filter all the incoming data. Few or all the special characters such as $, @, % should be avoided. Programmers should encode the output based upon input parameters [86].

5.4.2 Insecure direct object references

Insecure direct object references is an attack which exposes key internal implementation objects such as database elements, files or directories to an unauthorized user or an attacker [44]. In a web application, once the request to retrieve information is made by an end user, a web page is generated; an attacker can simply change the value of the parameter in the browser which refers to another object, and can simply access unauthorized information.

This security risk can be avoided by avoiding the use of direct object references. Having an indirect reference to objects can guard object references and which makes extremely difficult for the attackers to predict the references and gain unauthorized access. For example, while populating a dropdown list, a developer can populate the table with content codes, rather than name of the contents which can be used to predict direct
reference to an object. Developers can also enforce access controls on the objects. A control environment should be implemented where user access should be authenticated and authorized before the use of the objects [44].

5.4.3 Security misconfiguration

The security misconfiguration attack is not restricted to one particular level for example server, database, etc. Misconfiguration in security can happen at the server, database or even framework level. In this case, the attackers keep looking for security flaws and gaps in the application to get unauthorized access to files and directories [45]. Since this type of attack is not restricted to a software development or database administration, detecting a gap in security functionality requires a joint effort of developers, architects, database administrators, solution managers and everyone else involved in the software development process. Attackers can access applications using inactive accounts, server logs and default passwords. In case of an active directory listing, attackers can find classes and objects and which can be used to reengineer the actual application code. Server misconfiguration can provide traces that can lead to an actual user of the system.

Periodic scanning and auditing of code for any security vulnerability can prove to be extremely helpful in avoiding any misconfiguration. Developers should update the application framework and should include the libraries that can directly affect the security functionality of the application. In case of setting up a new environment, all the setting should be similar for development, QA and production so that any new software update is reflected in all the other environments [45].
5.4.4 Sensitive data exposure

This vulnerability denotes the stealing of sensitive data by gaining unauthorized access to the application. Data refers to browser data, backups or even the data in transit. Even though the data have been secured using different techniques, attackers try to find some flaw in the security measurements. For example, attackers try to find if a weak key generation algorithm has been used in the application which uses cryptography [46].

To prevent this vulnerability, developers should classify and encrypt all sensitive information that can be targeted by malicious users. Instead of storing the data, the application should only remember the data that has been classified as the least important information. Developers while coding the applications need to follow cryptographic algorithms with strong key management system [46].

5.4.5 Missing function level access control

Missing function level access control refers to attacks where attackers request access to some functionality of the application. In general, applications make a functionality available for users after verifying the access rights; however due to missing access control checks on the server, attackers can gain privileged access to unauthorized functionality [47]. An example of this type of security flaw is authenticated access for an under-privilege user.

Separate authentication module should be developed by the programmers which should be invoked by all business functions. Hard coding should be avoided. Access control lists should be used in protecting the application and all the default access should
be denied and access roles should be assigned according to the requirements. Access to URLs should also be denied, only the URLs that pass the vulnerability check should be accessed [47].

5.4.6 Weaknesses in authentication and authorization

Without proper authentication and authorization security measures, a user can easily attack an application and access sensitive information [48, 49]. Security weaknesses include flaws in areas such as password management, timeouts, secret questions and answers, account information, etc. In authentication attacks, attackers impersonate someone else and retrieve critical information [49]. Weakness in authorization lets an attacker access sensitive content and functionality of the application. Sometimes, depending upon the level of authentication, the user can also gain complete control of the application [49]. This type of attack can be easily carried out when access roles are not defined for the users and also when incompetent user name and password policies are used. Following user name and password such as abcd or 1234, can often lead to fast and easy access to application or even servers. However these authentication mechanisms prove to be easy for attackers to break as well.

These risks can be avoided by ensuring complex user name and password creation system. Developers should ensure the safety of username and password of all the users of the applications by developing security modules and applying cryptographic algorithm to the application code. Also programmers should define the access roles to ensure appropriate user privilege to the system.
5.4.7 Use of hard-coded credentials

Hard coding in the application development process is considered a very common flaw, however this flaw can have a very negative impact while running the software. Sometimes developers tend to hard-code information such as passwords, access codes, and cryptographic keys in the application [42]. This common flaw becomes a major vulnerability when the same access codes used throughout the application become visible and therefore make the client vulnerable. Exploiting hard coded credentials has been a very popular method among attackers and has caused extreme damage; for example, in 2010 the Stuxnet worm used hard coded credentials to disrupt the regular operation of Iranian nuclear sites and damaged their nuclear programs [51].

To avoid the risk from hard coded credentials, developers should apply proper authentication and cryptographic system to safeguard the credentials. Monitoring tools should be used by the programmers which can examine the application flow along with its interaction with operating system and the network. The behavior of the application should closely examined by the programmers and testers against any kind of fixed input string [87].

5.4.8 Invalidated redirects and forwards

Providing links on web pages is a common functionality implemented while developing a web application. Users find links on the web sites that redirect them to a new page. In most of the cases the links lack any validation and therefore a single click on a link can redirect a user to some phishing and malware sites [42, 52]. Sometimes
these redirected sites look legitimate, tricking the user into sharing private sensitive information.

Developers can prevent this type of risk by avoiding any kind of redirects in their code. However if any redirects is used, the user parameters should never be involved in calculating the destination. Developers should always use the mapping value of the destination instead of using an actual destination URL so that in case of an attack, the attacker should not be able to translate the mapped value to its actual URL [52].

These are few of the most common vulnerabilities found among applications. Developers and various organizations have developed secure coding standards for programmers so that they can be used to produce quality code along with proper security functionality.
Chapter 6

How Programmers Can Write Secure Code

This chapter will highlight different methods programmers can adopt to write secure code. Section 6.1 will explain some background information on the requirements for secure coding and Section 6.2 will highlight resources that can be useful for the programmers in producing secure code.

6.1 Background

In chapter 5, this paper explained why secure coding should have paramount importance. It explains how and why various sections of business including any public or private enterprise needs security. It explained what are the common errors and security flaws in applications and different security standards, guidelines and best practices that can be followed to eliminate any security vulnerabilities.

As the previous chapter presented, programming is the foundation of software development. Applications can be designed using a secure architecture, and they can be secured by taking various proactive and reactive measures. Security can be embedded in the application in the later phases, however the secure software development process will still require developers to program the application following all security parameters.
6.2 Programmer’s Resources

To achieve the goal of creating secure applications, organizations and programmers can adopt several proactive and reactive measures. Some of them are as follows:

1. Security oriented courses and specialized degrees
2. Security certifications
3. Organizational training and security programs
4. Online resources
5. Static code analysis and analysis tools
6. Security audits

6.2.1 Security oriented courses and specialized degrees

Since a high percentage of security incidents result from badly written code, learning a proper way to code is a very important task [56]. Programmers need to know the impact of insecure coding and how they can write good quality code along with proper security parameters. Most of the time students learn the basics of programming in their high school years, later on these students continue to learn programming at college and university level and finally in the work place environment. The learning process continues because of the ongoing development in technologies.

Most of the programmers lack the knowledge of security issues and do not understand the impact of possible threats. A few of the main reasons are that at college and university level, neither are there security oriented programs nor do the Computer
Science, Software Engineering and Information Technology programs include enough content on secure application development [56]. Students do not know enough about security and hence they pay no attention to security vulnerabilities in their code. Learning about application security alongside basic programming concepts can prove to be a proactive measure in the fight against cybercrime. Security oriented education can make the programmers aware of various security vulnerabilities and threats and errors. Apart from coding, these courses can educate programmers on various testing procedures, so that they can find and eliminate any security related issue. In some cases, even after applying adequate security parameters, absolute security cannot be achieved, but at least proper knowledge can help the developers write code which can be responsible for fewer security breaches. Similar to the courses, specialized degree programs should be created. Specialized degree programs can help students understand security from the very basics. The courses of the security degree should concentrate upon software security and information assurance. These degrees can help organizations in selecting the candidate with the appropriate specialty as needed.

A successful course module has been prepared by professors and teachers of the Computer Science department at North Carolina A&T State University [56]. The proposed module is divided into Introduction, Computer Security, Concepts, Insecure Code, Safe Programming Practices and Laboratory Exercise. These five modules cover and explain a variety of concepts including syntaxes, validation concepts, the need for and advantages of secure programming, and how these can be used in developing real time applications. Comparing a pre and post survey after completion of this module by a
number of students proved that a systematic curriculum dedicated to secure software development can be extremely helpful [56].

6.2.2 Security certifications

Programmers, either students or professionals, can obtain certain security certifications relevant to their field and their level of interest. A certification should never be the only criterion for working in software security; however it can be an influential factor. According to Grady Summers, America’s leader in information security program management services at Ernst & Young “in this era, a security certification is equivalent to a university degree and can be an important factor in hiring” [57].

Certifications give individuals a proper understanding of security. Looking at various attacks over the past decades, several organizations have developed courses and certifications for software professionals. These certifications are aimed at individuals working in this highly complex field. Based on the study of Charles M. Ray and Randy McCoy, the benefits of certifications can be categorized under three headings [58]:

1. Employer: An employer might enjoy the following benefits from hiring an employee with security certification.
   a. A certified employee can be more efficient and productive.
   b. Certified employee might require less or sometimes no training at all, hence saving on training time and money.
   c. A certified employee has better problem solving skills, especially in case of a serious situation.
2. Education: Certification not only provides assessment criteria for an individual, but it also helps in enhancing knowledge and providing insight into security vulnerabilities.

3. Student: Certifications can be helpful for students as well. For example, possessing an organization recognized certification can create multiple job opportunities for students.

Depending upon their functionality and their operation areas, certifications can be divided into two categories [58]:

1. Administrative: These certifications should be achieved by professions who tend towards administering the applications, network connections and data bases such as CISM, CISSP, CISA [58, 59, 60, 61, 62].

2. Technology: These certifications involve technical certification, mostly for programmers. For example CEH, GSSP-JAVA, GSSP-.NET, ESCP.NET [58, 63, 64, 65, 66].

6.2.3 Organizational training and security programs

Training sessions can be a very important factor, especially for new employees. With the huge changes in technologies, it is not necessary that individuals already are well trained on the product the organization is working on. Similar to training on technologies, enterprises should organize training sessions on security for fresh as well as experienced programmers. Such training can be useful for educating employees on secure coding, vulnerabilities, threats and various precautionary measures programmers can take.
to avoid these shortcomings. These sessions can also be used to educate and motivate programmers on language specific, general and project standards and security policies. Along with these, programmers can be introduced to secure coding standards and programming practices developed by organizations such as OWASP, CWE and Microsoft.

Together with security trainings, organizations should have a dedicated security department, which should oversee all the development. One of the major roles of this department should be to help programmers and managers produce secure applications; however it should always be accessible to programmers regarding any security enquiry that can prove to be helpful in developing secure software.

6.2.4 Online resources

Development in technologies has also resulted in development of resources to help individuals. Similar to other off-line resources such as classes and training programs at university, programmers also have access to various online resources. These online resources can be categorized as follows:

1. Blogs: Blogs are basically personal websites where users discuss or express their opinions on different subjects. Security professionals and programmers discuss common programming and software related issues through these web casts. For developers especially new programmers, these websites can be very informative.

2. Online courses: Programmers can learn about secure coding by taking various online courses. Universities and standard organizations such as Stanford
University [67] and SANS [68] provide various online courses for students and working professionals.

6.2.5 Static code analysis and analysis tools

Static code analysis is one of the most popular and important measures programmers take to identify the pitfalls and various security shortcomings in their code. With the help of automated tools, these static analysis processes analyze the code for errors and vulnerabilities without executing the program [72]. The static analysis approach helps in reviewing the code, checking for compliance with secure code and quality code standards [73]. The analysis is done manually or with the use of analysis tools, however analysis tools save a lot of time for the programmers as well as providing several suggestions and examples of how programmers can fix the vulnerability.

These tools integrate security standards, general standards and quality code development standards. With continuous change in technology and various security standards, programmers might not be aware of current vulnerabilities. With the help of the analyzers, programmers do not need to be aware of every standard [73].

Static analysis tools are fast and efficient and extremely helpful for original authors and other programmers, especially in the testing phase. Testing the application for security related issues can be a very complicated task and might require immediate attention. In the case of the unavailability of the original author of the code, finding the bug and correcting it can be a time consuming process. Static code analysis tools can test the application while the author is writing the code and in the case of the unavailability of
the author, it can direct a programmer to the section that needs some work. Also these tools provide guidance and references and sometimes sample code for the developers to follow. Hence using the tool not only reduces the time of development but also reduces the number of errors in the software. They significantly affect the software development process [73].

The software industry is not limited to one technology, in fact based on the technology and language used for development, several static analysis tools have been developed. These tools include their own rules for framework, application design, libraries, etc. [73]. A few of the most popular static analysis tools are [74, 75, 76, 77, 78, 79, 80, 81]:

1. FxCop
2. CodeSonar
3. CheckMarx code analyzer
4. HP Fortify Static Code Analyzer
5. Parasoft dotTEST
6. Parasoft Jtest
7. CodeIt.Right
8. Coverity SAVE

6.2.6 Security audits

Security audits, particularly source code audits, involve sets of code security checklists which can be used to identify and reduce the number of vulnerabilities in
software [69]. Source code audits analyze the code and on the basis of security measures, vulnerabilities are detected. The original authors are also involved in the audit so that if needed, changes can be assigned to the author instead of to a new developer.

The code audit process includes detecting all manipulatable entries such as various I/O entries, network input entries, etc., checking all security properties along with any possible exploitable weakness, generating warnings and errors if necessary and providing suggestions to programmers on how to fix the application [71]. With the help of code audits, programmers can check for all the exploitable content in the code and changes can be done to the code accordingly.

By using these methods the software industry can help programmers to produce high quality, secure applications.
Chapter 7

Conclusion and Future Work

7.1 Conclusion

Infrastructure security is directly affected by the security of cyber space and its components. The inclusion of computerized components for processes such as command and control can be recognized in all critical infrastructure sectors. The high usage of computer and software applications have highly impacted today’s working culture. Today with the usage of computer and software technology, tasks can be achieved in a much simpler and easier way. For example, infrastructure sectors, such as energy, health and transportation, use computerized components and cyber space to accomplish several tasks. But with the technological change to using cyber space, new types of security threats were created. Through cyber-attacks, cyber criminals and cyber terrorists can disrupt and damage the regular functioning of critical services without getting in direct contact with the target. Protecting critical services involves a combined effort of political, strategic and technical aspects, which also includes users from those areas.

This report highlights the significance of the cyber world in this technological era and explains the importance of cyber security. The software development process is one basic yet extremely important part of the technical aspect. According to several researchers, one of the basic reasons for so many cyber incidents is software which is insecure and has been developed without using any security parameters. This report explains how the secure software development process can contribute to securing cyber
space and why the role of a programmer in this process is extremely critical. This report justifies the need and necessity of secure applications and explains why programmers need to follow secure development standards produced by organizations such as OWASP and CWE. These organizations prepare vulnerability check lists every year, in which they explain critical software flaws, vulnerabilities and guidelines by which software developers can eliminate those vulnerabilities and security threats. Software vulnerabilities and security threats need to be addressed and reactive security measures need to be implemented accordingly.

This report explains cyber space in detail along with its relation to critical infrastructure. Several issues regarding cyber space and its relation to the software development process have been addressed in this report. This study also raised a few unanswered questions. Following are a few areas which need immediate attention and work should be pursued accordingly.

Firstly, in the process of making critical infrastructure secure, a governing committee of a nation needs to put extra attention towards creating proactive measures. They need to understand the role critical infrastructure plays in the proper functioning of modern society and why they are tempting targets for cyber criminals and terrorists. Physical as well as technical awareness programs should be arranged for all the actors. These programs should explain the precautionary measures that should be applied in case of a cyber-attack, especially ones targeted towards critical infrastructure.

Secondly, programmers need to understand their role in the software development life cycle. Programmers have the responsibility for creating secure applications and
therefore they should be prepared for this job accordingly. Universities should introduce new and advanced courses on security targeted towards computer, network, mobile and cyber securities. Apart from education, software organizations should provide appropriate training and information sessions for software developers.

Finally, every computer and cyber space user should be made aware of the risk of insecure cyber space and the threats it poses to society. Today, computer and the internet users can be of any age; they can be high school students and they can also be senior citizens. Governments along with educational institutions should develop programs for users of all age groups, which should teach and explain basic information about computers, mobiles, the internet and how users can secure themselves from cyber criminals and cyber terrorists.

7.2 Future Work

As mentioned earlier, the objective of this report is to highlight various threats to critical infrastructure and cyber space and its impact on the society. This report also aims to promote awareness about the unintended software flaws and vulnerabilities which occur during the different phases of the software development life cycle; especially during the programming phase. Besides publishing this report, I intend to consolidate this report into a slideshow and series of lectures to be presented in information sessions and seminars at educational and technical institutions such as colleges, universities, IT companies and software firms. Further, I also intend to develop a website with detailed collection of information presented in this report; and use this report and sample code to illustrate how badly written code is and can be exploited. I also aim to explain the need
and necessity of code analyzers and explain how code analyzers detect programming errors and vulnerabilities. Further, with the help of sample code, I would like to illustrate how an organized code-writing approach could minimize the security threats and loopholes. A series of video lectures with the said illustrations could be added to the website to make the knowledge transfer more efficient.
Bibliography


94. KULESZ, KAMIL, and ZBIGNIEW KOTULSKI. "Countermeasures against Traffic Analysis for Open Networks." 2005, 1, 3, 4.
http://cseweb.ucsd.edu/~clbailey/PortScans.pdf.
Curriculum Vitae

Candidate's full name: Bijiteshwar Rudra Aayush

Universities attended: Bharati Vidyapeeth University, B.E Information Technology, 2009

Publications: No Publications

Conference Presentations: None