Information Security Lab

15B17CI576

Odd 2023

Week 1(28th July – 3rd August)

Note: Students are advised to submit their solutions to respective lab faculty. The solution file must be named as "rollno_first name_w1.doc" (here w1 represents week1).

Information security is the practice of protecting information by mitigating information risks. It involves the protection of information systems and the information processed, stored and transmitted by these systems from unauthorized access, use, disclosure, disruption, modification or destruction. This includes the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms.

Why we use Information Security?

We use information security to protect valuable information assets from a wide range of threats, including theft, espionage, and cybercrime. Information security is necessary to ensure the confidentiality, integrity, and availability of information, whether it is stored digitally or in other forms such as paper documents. **Here are some key reasons why information security is important:**

- Protecting sensitive information
- Mitigating risk
- Compliance with regulations
- Protecting reputation
- Ensuring business continuity

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

Confidentiality – means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.

Integrity – means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

Availability – means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.

Here are some recommended reference materials for information security:

- "Handbook of Information Security, Volume 1" edited by Hossein Bidgoli
- "Information Security Principles and Practice" by Mark Stanislav and Mark Merkow.
- "Computer Security Fundamentals" by Chuck Easttom.
- "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman.
- The National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- ISO/IEC 27001 Information Security Management Systems Standard.
- SANS Institute, which offers a variety of information security resources and training programs.
- OWASP Foundation, which provides information and tools to help organizations improve their application security

---

Note: Read the help file on classical encryption for explanation of ciphers in this lab.

1. **Explore some websites and mention about its purpose :**
    - https://10minutemail.com/
    - https://www.whatismyip.com/
    - https://www.tracemyip.org/
    - www.ip2location.com
    - www.ipfingerprints.com
    - www.imei.inf
    - www.ceir.gov.in
    - https://timeline.google.com/maps/timeline
    - https://takeout.google.com/
    - www.haveibeenpwned.com
    - www.intelx.io
    - www.truecaller.com/unlisting

2. **Explore the following terms with respect to information security:**

- Cryptography
- Cryptanalysis
- Attacks
- Encryption/decryption
- Plain text/ cipher text
- Key: symmetric /asymmetric

3. **Explore following classical symmetric key encryption techniques:**

- Substitution encryption
    1. Caesar Cipher
    2. Monoalphabetic Cipher
    3. Playfair Cipher
    4. Hill Cipher
    5. Polyalphabetic Cipher
    6. One Time Pad
- Transposition encryption
    1. Rail fence cipher

4. **Understand the following codes and examine which encryption techniques are used:**

CODE1:

```
#include<stdio.h>
#include<conio.h>
 #include<string.h>
void main()
 {
intkey,i;
char data[30];
clrscr();
printf("\nEnter the plain text: ");
gets(data);
printf("\nEnter the key value: ");
scanf("%d",&key);
for(i=0;i<strlen(data);i++)
 {
if(data[i]!=' ')
 {
if(data[i]>= data[strlen(data)-1-key])
 {
data[i]=data[i]-26;
 }
data[i]=data[i]+key;
 }
 }
printf("Your cipher text is: %s",data);
getch();
 }
```

CODE 2:

```
#include<stdio.h>
 #include<conio.h>
 #include<string.h>
void main()
 {
char s[30],k[27],c[30];
inti, index;
clrscr();
printf("Enter plain text: ");
gets(s);
printf("\nEnter key with 26 character:");
for(i=0;i<26;i++)
 {
printf("\n%c",i+97);
k[i]=getch();
printf("%c",k[i]);
 }
for(i=0;i<strlen(s);i++)
```

```
 {
index=s[i]-97;
c[i]=k[index];
 }
printf("Your cipher text is:");
for(i=0;i<strlen(s);i++)
 {
printf("%c",c[i]);
 }
getch();
 }
```