IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735. Volume 5, Issue 1 (Jan. - Feb. 2013), PP 60-64
www.iosrjournals.org

Using Mono-Alphabetic Substitution to Secure Against Threats and Risk in Information Technology

G. I. Ighalo[1], T. E. Ighalo[2] and B. S. Ighalo[3]
Ambrose Alli University, P. M. B. 14 Ekpoma- Nigeria

Abstract: The awareness the world over on information technology (IT) is a welcome development but calls for great care and concern. This is so as there are out there, many people with evil minds who see nothing good that they would not capitalize on. There are persons who would want to create problems to make systems not workable while there are others who would want to steal or destroy such systems.

This write-up therefore tries to analyse information technology systems, looking at all possible threats and risks and how to combat or make such systems secure. In doing this, very simple yet difficult to guess systems software are designed to check evil practices such that would-be risk or threat persons would find it difficult to use. Encryption methods that use either the substitution or transposition principles are designed to protect such threats or risk. The written program will encipher and decipher information such that the integrity of the information is protected. This method chooses this enciphering and deciphering such that any user can easily learn and design his/her own keys which are not stored in the system. Other measures that will check threats and risks are proposed and counter measures that are involved with access control are provided. A better risk management and training are proposed.

Keywords: *cipher, integrity, risk, substitution, threats, transposition*

I. Introduction

Problems associated with computer systems and applications are privacy and security. Any network or even individual computer system without provision for privacy and security paves way for possible threats. Computer systems contain personal data and are accessible from distant terminals. When this situation arises, worms and viruses could be transmitted to such free systems with ease. Software obtained from such external sources provides a means of security risk [1].

A threat to a computer system is any potential occurrence malicious or otherwise that can have an individual effect on the assets and resources associated with the system. Threats can be reduced in any system by identifying and removing vulnerabilities. Vulnerabilities make systems more prone to attacks or they make attacks more likely to have success or impact. However there are countermeasures for vulnerabilities. These could be classified into four main types:

- Deterrent controls: These types tend to reduce the likelihood of a deliberate attack.
- Preventive controls: These types protect vulnerabilities and make any attack unsuccessful or reduce its impact.
- Corrective controls: they reduce the effect of an attack
- Detective controls: these types discover attack, and alerts or triggers preventive or corrective controls [2].

Threats to computer systems can be described in three forms:

(a) **Disclosure threat** – When information is passed onto a person that it was not meant then it becomes a disclosure threat. This can be referred to as a leak. This situation arises when some secret stored in a computer system is disclosed to someone to whom it was not meant (e.g. instructions for building a nuclear bomb)

(b) **Integrity threat –** This involves any unauthorized change to information stored in a computer or in transit between computer systems. Also entry of false information or data to computer systems can be seen as involving life or loss of information.

(c) **Denial of service: -** When access to some system resources is blocked intentionally then it implies denial of service. This blocking may become permanent

Many other threats to information technology can be described in the form of computer crimes, cyber crimes, fraud etc. These types of threats have led to loss of billions of dollars. Most of these threats lead to breakdown, taking wrong decisions due to alterations [3]. To understand the issue of risk in information technology, it is of the view that various institutions using information technology systems must study their various organizations properly. They need to undergo various management problems especially as it relates to its technology. For any good security measures to be effective on the risk and Threats in IT, it would require a proper study on all such systems. Such study would include **access control, network security, data integrity, asset management and software acquisition and development [4].**

It is common knowledge that most of the breaches in IT originated from inside of the various organizations. In the US, it is documented that 45 percent of US organizations polled reported unauthorized access by insiders. In addition, financial fraud and theft of proprietary information – "opportunity crimes" that securities experts say require access to company systems and insiders knowledge – ranked as the most costly types of computer crime. To help mitigate the risk of both deliberate and unintentional damage, organizations need to establish effective access control measures. Also policies and procedures that clearly define individual responsibilities for supporting or changing the computing environment need be established.

II. Materials And Methods

One of the foremost measures in checking risk of threats against IT is the access rights granted to all workers of any organization. Granting employees too many views enables them to extrapolate or conjecture further on information and exploit confidential data. The degree of access control depends on the value of data being protected. Many organizations use passwords for access control. For more sensitive information, it may require more rigorous measures such as biometric scans, smart cards, or one time password devices. Auditors in well established organizations are used to help determine the degree of control necessary by evaluating the risk facing each system. It has been found that when passwords are used, the most common form of access control is commonsense questions which have yielded very good results. Generally risks are defined and categorized. This definition creates or allows cost effective security measures to be employed and hence a consequent reduction in the risk gap. There are risks which need to be addressed by countermeasures, there are those that can be accepted and there are those to be insured against. As the IT revolves around the computer application then issues of security measures implies the security of computer systems. There are two types of computer security measures to be considered-

- **Physical security measures, and**
- **Logical security measures.**

Physical security measures – These types of measures are external to the hardware and software systems. They are intended to prevent or facilitate recovery from physical disaster such as fire, flood riots, sabotage and theft of physical resources. These include control of physical access to computing resources in order to make decisions about who can have access to each terminal or user accounts as well as to the computer room itself.

Logical security measures – these types are internal to the computer system. In these types of measures, actions are taken before and after a threat have occurred. **Countermeasures** here prevent threats that have already occurred. **Safeguards** are placed to prevent having effects of known threats. Countermeasures and safeguards which when built in any system will perfectly keep good security is:-

i) Auditing and intrusion detection
ii) Identification and authentication
iii) Encryption
iv) Mandatory and discretional access control
v) Privileges
vi) Security kernels
vii) Configuration management
viii) Format specification and verification
ix) Enhancing life circle activities

Presently, there are a lot of developed security measures which can be applied to secure information's in information technology. One of such developed packages is that by IBM (International Business Machine) which introduced the electronic copyright management system that uses a secure packaging technology called enable owner of copy righted material to distribute their information securely over the Internet and receive payment use. Another such method is that using a combination of software encryption and unique laser treatment to make copying of CD-ROMS immensely difficult. This system is embedded into each CD-ROM. At the mastering stage, each CD-ROM has a unique locking code that provides protections at three levels. The end result is that the products cannot be copied by any currently available CD recordable machine.

The security implementation in this paper is based on the basic security of any information system which is :- (a) identification authentication
(b) Authorization (access control)
(c) Integrity, consistence integrity constraint and rules been applied.

Atypical encryption programme was carried out to execute the security process. The program is written using mono-alphabetic substitution as a security measure. It does not require any key to encrypt or decrypt a message and it is not complex. The presenter has been guided by the fact that many persons do not understand basic mathematics and this approach has been chosen such that any individual can design his or her own mono-alphabetic substitution security measure.

A typical security measure that can be used by owners of small scale enterprise is the format shown in the program highlighted hereunder. As soon as the private entrepreneur opens his computer with his password, so long as the programme has been installed, he needs to close his programme. This will enable him or her to execute his normal work in the normal language, be it in English or any language. As soon as he finishes, he can allow his programme to run and encrypt the work he has just typed or executed. He can then live his work in the encrypted format or close the work. This process may be tedious but for security it is necessary. The programme for the decryption mechanism is written in Pascal.

III Program

This program can be used encipher a message of interchanging by cipher alphabet and real alphabet

```
PROGRAM DECIPHER MESSAGE (INPUT, OUTPUT)
        This program deciphers a message, which has been coded using the
Non-alphabetic substitution code.
USES CRT
CONST
ALPHABETLENGHT  37,
MAXLEN = 80;
TYPE
ALPHABET = ARRY [1 ALPHABETLENGTH] OF CHAR;
CHARLINE = ARRAY [1, MAXLEN] OF CHAR;
{Procedure asks user to either read and cipher alphabets for the deciphering}
Var
IndeX: integer;
Begin
Clrser;
        Writeln (‘please enter the real alphabet’)
        FOR index =  1 To alphabet length Do
        Read (Real A1 [index]); Readln;
Writeln (‘Below each letter in the real alphabet, please enter);
Writeln (‘ the corresponding letter of the cipher alphabet);
FOR index = I TO alphabet length Do
        Write ( real AI (index) writeln
FOR index = 1 TO alphabet length DO
        Read ( cipher A1 (index); readln
End : Enteralphabet);
Procedure Enterline (var codedmess: charline codelen in integer):
(procedure enters the coded message to be deciphered)
Var
begin
Writeln (please enter your coded message)
        Codelen; = 0,
WHILE (not EOLN) and Codelen & maxlen) DO
Begin
        Codelen = Codelen + 1:
        Read ( codedmess (Codelen).
End;
IF NOT EOLN THEN
Writeln (‘your coded message was too long; “message truncated to”
Maxlen: 1,; characters’); readln
End {Enterline}:
Procedure Decipher ( var code:  charline; plain;
Charline, length: integer; real A1,
Charline A1: alphabe),
Procedure deciphers coded message; looking up letter in the cipher A1 and
using the corresponding letters in real A1 to get the plain message.
Var
Index, position integer.
```

```
Procedure find { the position of the letter in the given alpha}
Begin
Position; = 1
WHILE ( letter alphabet [position]) Do
        Position : = position  + 1

        End  { find}
        Begin {Decipher }
        For index:  = 1 TO length DO
        Begin
        Find ( position, code [ index ], cipher A1),
        Plain [index];  =  real A1 [position ]
End
End  [decipher]
Procedure print-results ( code, message charline length integer
{ This procedures print the message and the resulting coded text}
Var
Index integer
Begin
Writeln (“when the coded message)
Read1n
For index: = 1 TO length DO
        Write (code [index])
Write1n; read1n
Write1n (is decoded with the above substitutions, the result is”)
For index:  = 1 to length DO
Write ( message [index ])
Write1n Read1n
End { print result};
Processing;
{ This procedure controls the main steps of data entry and processing}
Var
Real alphabet, Cipheralphabet; alphabet,
Message, Codedness: charline;
Input1en: integer;
Enteralphabets (realalphabet, cipheralphabet)
Enterline ( codeness, input1en);
Decipher ( codedness, message, input1en,
Realaphabet, cipheralphabet);
Printresults ( codedness, message, input1en)
End { control processing};
Begin { of main }
        Write1n (‘Deciphering program’)
        Control processing
End { of main }
```

IV Using This Programme

This typical programme has been written to encrypt and decrypt information already stored in any computer system. It makes all information stored in a computer system not accessible to any user except the owner or any person authorized to use such system as he/she has the password to open such system. If this programme is enabled after a user enters his/her password access is given to the user automatically. As soon as he/she finishes with the work at hand he/she can then encrypt the work before closing the system. In so doing, the work in the system becomes encrypted until a decryption process is enabled. The entire work on the computer becomes encrypted and secured from any intruder. In addition a process whereby an unauthorized attacker is only allowed two attempt after which it becomes locked and any other attempt is seen as an error.

V Conclusion

The encryption techniquehereto demonstrates that information can be kept secured to a certain extent so far the process is known to all and sundry. This encryption technique will mitigate the threat and attack faced by computers. Alphabetic substitution does not require the use of keys, but can protect information from any how attack. Other methods of encryption can be used to keep information secured. Constant changing of encryption methods can continuously keep information secured. Other Programming languages could also be used.

References

[1] Bowker Sauer C. (1993) “Security of electronic information perspectives in information management

[2] Parker D. B. (1982) “Computer security some easy things to do”. Wellesley Publishing co.

[3] Burham D. (1983), “The Risk of the computer state”. New York; Random House

[4] John Silltow (2003) Shedding light on information technology Risk: Business services Industry

[5] Thomas L. Naps (1988) Programme Design with Pascal; West Publishing Company, New York