A Result Paper-Network Vulnerability Scanning

Swati Rohillal[1], Santosh Kumar Singh[2]
Student, Jind Institute of Engineering & Technology, Jind,India[1], swatirohilla95@gmail.com[1]
Professor, Jind Institute of Engineering and Technology, Jind, India[2], singhsantosh1201@gmail.com[2]

ABSTRACT:- Objective of research is to preserves the secure condition it is essential to be aware of the behavior of the incoming data. It is a too vulnerable and complicated Question. Owing to the fact that intrusive data are in several and similar forms, distinguishing them from the normal ones is so outstanding. Network Security is becoming an important issue for all the organizations, and with the increase in knowledge of hackers and intruders they have made many successful attempts to bring down high-profile company university network sand web services.

ISSN : 2348-5612 © URR
9 770234 856124

[1] INDRODUCTION

Network University Security

Computer network is a collection of autonomous computer interconnected by a single technology. A Computer Network is often refers to as a network, is used to share resources, applications and information through devices connected to the network. The computers are said to be interconnected if they are able to exchange information. The connection need not be a copper wire, fiber optics, microwaves, infrared and communication satellites can be used. Networks come in many sizes, shapes and forms. The issue here is resource sharing and the goal is to make all programs, equipment and especially data available to anyone on the network without regard to physical location of the resources and the user. There are two types of computer network configuration, client/server networks and peer-to-peer networks. Client/server networks are more suitable for larger networks. Peer-to-peer are commonly implemented where less then ten computers are involved and where strict security is not necessary.

Need of Network Security

There are great numbers of threat to a network's security; there are fortunately many preventative techniques to properly secure at work against those threats. There is some of the fact about the network security.

1. Increasing complexity of computer infrastructure administration and management.
2. Decreasing Skill level needed for exploits.
3. Direct impact of security breach on corporate asset base and goodwill.
4. Increased networks environment and network based applications.
5. Evolution of technology focused on ease of use.
6. Evolution of technology focused on ease of use.

A major security objective is measuring the costs and benefits of security. If the cost is to be measure for securing an entity, whether it is data on networks, data on computers, or other assets of an organization, something has to be known about risk assessment.

Importance of a Security Policy

Security policies provide many benefits and are worth the time and needed to develop them. Security policies are important to organizations for a number of reasons, including the following:

1. Create a baseline of your current security posture.
2. Set the framework for security implementation.
3. Define allowed and disallowed behavior.
4. Help determine necessary tools and procedures.
5. Communicate consensus and define roles.
6. Define how part oh and security incidents.

[2] LITERATURE SURVEY

Vulnerability has been discussed in brief University in the previous chapter, however if we go through the literature, we came to know about the r s archers who have previously worked upon this topic. How to overcome from vulnerabilities, what are the major types of vulnerability, detection of the arability. ACO has been in the spot light for almost two decades, many of the work have been done in this field by researchers. Ant Colony Optimization as the name suggest is he problem for finding out the optimal result. Started in the early 90s, a researcher Marco Dorigo, during his Ph.D thesis, came to know about the behavior of the real Ants, how they came to know about the food from the nest, and how they communicate with each other to tell other where the food is. Marco with his colleague name Di Caro and Gambardella have worked upon Ant Colony Optimization. Vulnerability in the system means having weakness in system. These weaknesses are greatly exploits by the hacker to gain access into your system. Any vulnerable system is open to the hacker they can do anything to your system. They can steal any type of information from your computer. Main cause of presence of any type of vulnerabilities in the system is due to lack of programming. And it is due to some flaws in the Software. When hackers came to know about this weaknesses about your system they can easily hook on to your system and can exploits them up to any extent. Some methods need to adopted to overcome from these weaknesses. Main cause of Vulnerabilities is as follows:

- **Complexity** : large, complex systems increase the probability of flaws and unintended access points.
- **Familiarity** : Using common, well-known code, software, operating system, and hardware increases the probability University an attack erhasorcan find the knowledge and tools to exploits the flaw.
- **Connectivity** : More physical connections, privileges, ports, protocols, and services and time each of those are accessible increase vulnerability.
- **Password management flaws**: The computer user uses weak passwords that could be discovered by brute force. The computer user stores the password on the computer Thapar where progam can access . Users re-use passwords between many programs and websites.
- **operating system design flaws**: The operating system designer chooses to enforce sub optimal policies on user/program/ management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer. This operating system flaw allows viruses and mal ware to execute commands on behalf of the administrator.

Fundamental operating system design flaws: The operating system de-signer chooses to enforce sub optimal policies on user/program/ management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer.

[3] TOOLS & TECHNOLOGY

CLIENT SERVER MODEL

It is possible for two network applications to begin simultaneously, but it is impractical to require it. Therefore, it makes sense to design communicating network applications to perform complementary network operations in sequence, rather than simultaneously. The server executes first and waits to receive; the client executes second and sends the first network packet to the server. After initial contact, either the client or the server is capable of sending and receiving data.

JAVA SOCKET PROGRAMMING

Java Socket programming has been used for communication btw applications running on different JRE.

Java Socket programming could be connection-oriented or connection-less.

Socket & ServerSocket classes are used for connection-oriented socket programming & DatagramSocket & DatagramPacket classes are used for connection-less socket programming.

PORT

Sockets are UNIQUELY identified by Internet address, end-to-end protocol, and port number. That is why when a socket is first created it is vital to match it with a valid IP address and a port number. In our labs we will basically be working with TCP sockets. Ports are software objects to multiplex data between different applications. When a host receives a packet, it travels up the protocol stack and finally reaches the application layer. Now consider a user running an ftp client, a telnet client, and a web browser concurrently.

Port	Service Name,Alias	Description
1	Tcpmux	TCP port service multiplexer
7	Echo	Echo server
9	Discard	Like/dev/nu11
13	Daytime	Systemsdate/time
20	ftp-data	FTP data port
21	ftp	Main FTP conection
23	telnet	Telnet conection
25	Smtp,mail	UNIX mail
37	Time,timeserver	TIME server
42	Nameserver	Time server
70	Gopher	Text/menu information
79	Finger	Current users
80	www,http	Web server

Table 3.1 Port Table

[4]PROPOSED WORK

We have discussion the proposed work in following step:-

Step 1 Get data from file and store in packet

Step 2 Perform xor operation on the data to encode

Step 3 Perform AES to encrypt the data

Step 4 Perform AES to encrypt the data

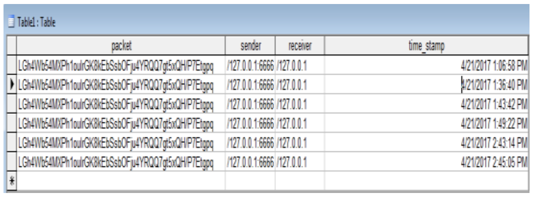
Step 5 Perform xor operation on the data to encode

Step 6 Get data from file and store in packet

[5] RESULTS & IMPLEMENTATION

Here we have to transfer lx.txt file from client to server. Here we have used java based socket programming in order to transfer packet from client to server.

Once packet is transferred the details of packets , sender ,receiver, time_stamp is stored in database file. If same packet is delivered over network within 5 minutes than packet cannot be sent thus same packet can be transferred after 5 minute of transmission in order to stop un authentic delivery of packet. This would also reduce the chances of unknowingly made retransmissions.

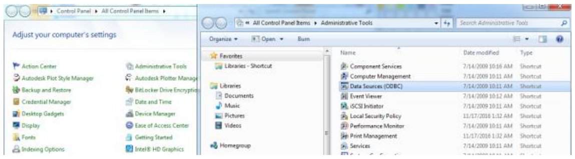


packet	sender	receiver	time_stamp
LGh4Wb54MXPh1oulrGK8kEbSsbOFju4YRQQ7gt5xQH/P7Etgpq	/127.0.0.1:6666	/127.0.0.1	4/21/2017 1:06:58 PM
LGh4Wb54MXPh1oulrGK8kEbSsbOFju4YRQQ7gt5xQH/P7Etgpq	/127.0.0.1:6666	/127.0.0.1	4/21/2017 1:36:40 PM
LGh4Wb54MXPh1oulrGK8kEbSsbOFju4YRQQ7gt5xQH/P7Etgpq	/127.0.0.1:6666	/127.0.0.1	4/21/2017 1:43:42 PM
LGh4Wb54MXPh1oulrGK8kEbSsbOFju4YRQQ7gt5xQH/P7Etgpq	/127.0.0.1:6666	/127.0.0.1	4/21/2017 1:49:22 PM
LGh4Wb54MXPh1oulrGK8kEbSsbOFju4YRQQ7gt5xQH/P7Etgpq	/127.0.0.1:6666	/127.0.0.1	4/21/2017 2:43:14 PM
LGh4Wb54MXPh1oulrGK8kEbSsbOFju4YRQQ7gt5xQH/P7Etgpq	/127.0.0.1:6666	/127.0.0.1	4/21/2017 2:45:05 PM

Table 1 to store packet ,sender,receiver , timestamp details

To connect java code with database we have to create dsn using following step:

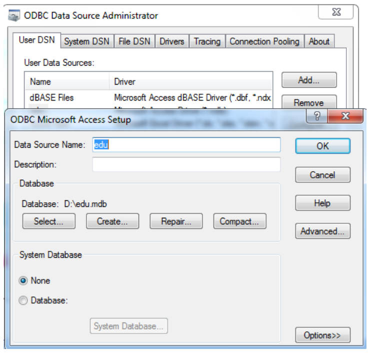
1. Open control panel
2. Go to Administrative tools
3. Click on data source (ODBC)



Name	Date modified	Type
Component Services	7/14/2009 10:16 AM	Shortcut
Computer Management	7/14/2009 10:11 AM	Shortcut
Data Sources (ODBC)	7/14/2009 10:11 AM	Shortcut
Event Viewer	7/14/2009 10:12 AM	Shortcut
iSCSI Initiator	7/14/2009 10:11 AM	Shortcut
Local Security Policy	11/17/2016 1:32 AM	Shortcut
Performance Monitor	7/14/2009 10:11 AM	Shortcut
Print Management	11/17/2016 1:32 AM	Shortcut
Services	7/14/2009 10:11 AM	Shortcut

Fig 1 Data sources in ms access

4. Click on add select driver for ms access
5. Select the path of database and set the name of dsn and press ok



User Data Sources:

Name	Driver
dBASE Files	Microsoft Access dBASE Driver (*.dbf, *.ndx

Data Source Name: edu

Description:

Database

Database: D:\edu.mdb

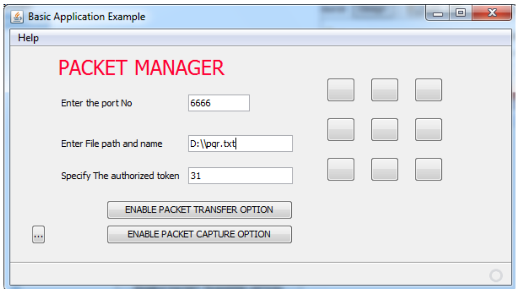
System Database

● None

○ Database:

Fig 2 the path of database and set the name of dsn and press ok

When we run server side module then we have to specify port no, file path and authorized token (for XOR operation), on Right side we get 9 button to create pattern in order to generate advance AES key. Then we enable packet transfer by clicking on "ENABLE PACKET TRANSFER OPTION"


Basic Application Example
Help
ENABLE PACKET TRANSFER OPTION
ENABLE PACKET CAPTURE OPTION

PACKET MANAGER

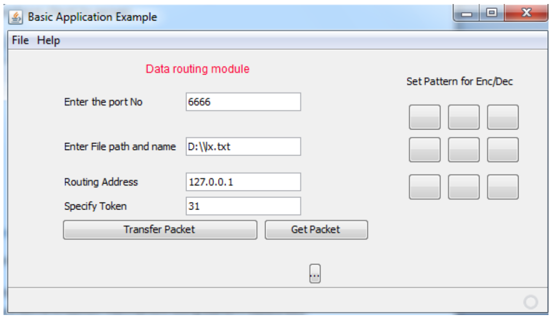
Enter the port No: 6666

Enter File path and name: D:\\pqr.txt

Specify The authorized token: 31

Fig 3 Enable packet transfer option

On Client side we specify the same port no along with file name and path with ip address of server and token (for XOR operation). Here same pattern for decryption is used that is present on server side. Then we click on transfer packet button.



Data routing module

Enter the port No: 6666

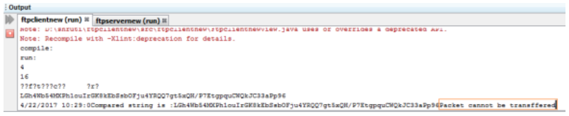
Enter File path and name: D:\\x.txt

Routing Address: 127.0.0.1

Specify Token: 31

Fig 4 Basic application

If same packet is not sent within previous 5 minutes then packet is transmitted and file is uploaded on server end.



```
Note: D:\shruti\ftpclientnew\src\ftpclientnew\ftpclientnewview.java uses or overrides a deprecated API.
Note: Recompile with -Xlint:deprecation for details.
compile:
run:
4
16
??f?t???c??     ?r?
LGh4Wb54MXPh1ouIrGK8kEbSsbOFju4YRQQ7gt5xQH/P7EtgpquCWQkJC33aPp96
4/22/2017 10:29:0Compared string is :LGh4Wb54MXPh1ouIrGK8kEbSsbOFju4YRQQ7gt5xQH/P7EtgpquCWQkJC33aPp96Packet cannot be transffered
```

Fig 5 Packet is transmitted and file is uploaded on server end.

After transmission of pqr the following data is shown in d: on server side.

If pattern matches and server and client side then data is decrypted otherwise information becomes non understandable to user. Click on the button in pattern must be done in order.

If pattern matches but order is wrong then decryption fails.

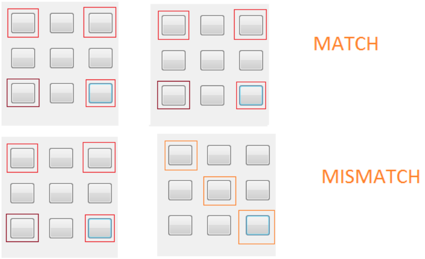


Fig 6 Pattern Matching

User defined XOR function

```
public String xor(String a,int b)
{
    StringBuilder sb = new StringBuilder();
  for(int k=0;k<a.length();k++)
  sb.append((char)(a.charAt(k) ^ b)) ;
        String result;
         result = sb.toString();
  return result;
   }
```

SOURCE CODE TO INSERT TIME STAMP

```
public static void ins(String a, String b, String c)

{

int flag=0;
try
         {

Class.forName("sun.jdbc.odbc.JdbcOdbcDriver"
);
         Connection
con=DriverManager.getConnection("jdbc:odbc:
edu","","");
         Statement st=con.createStatement();
         java.util.Date date=new java.util.Date();
   //System.out.println(date);
 Calendar cal = Calendar.getInstance();
cal.setTime(date);
int year = cal.get(Calendar.YEAR);
int month = cal.get(Calendar.MONTH)+1;
int day = cal.get(Calendar.DAY_OF_MONTH);
int hour = cal.get(Calendar.HOUR_OF_DAY);
int minute = cal.get(Calendar.MINUTE);
int second = cal.get(Calendar.SECOND);
          st.execute("insert into table1 values('" + a
+ "','"+ b + "','"+ c+"','" + month + "-" + day + "-
" + year + " " + hour + ":" + minute + ":" +
second + "')" );

st.close();
          con.close();
        }
catch(Exception e)
{
System.out.println(e);
}
```

Code to check the Validity of packet

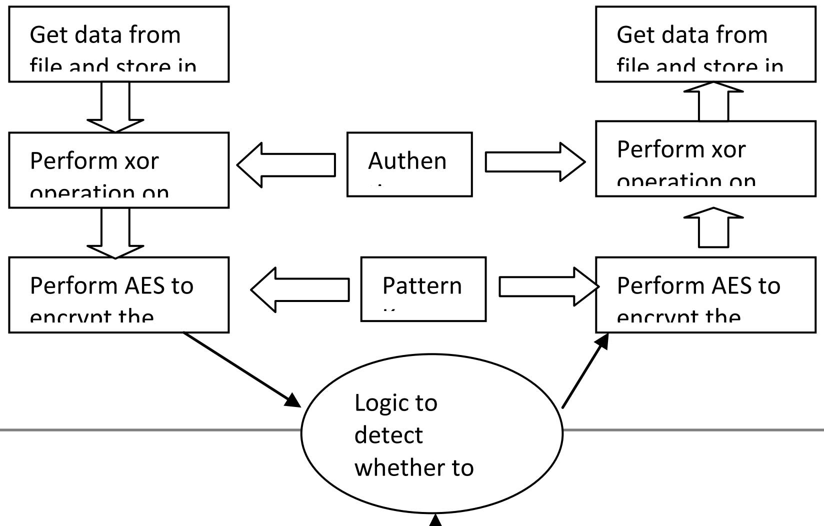
```
public  static int  isvaidpacket(String dd)
{
int flag=0;
try
          {

Class.forName("sun.jdbc.odbc.JdbcOdbcDriver"
);
          Connection
con=DriverManager.getConnection("jdbc:odbc:
edu","","");
          Statement st=con.createStatement();
           java.util.Date date=new java.util.Date();
   //System.out.println(date);
 Calendar cal = Calendar.getInstance();
cal.setTime(date);
int year = cal.get(Calendar.YEAR);
int month = cal.get(Calendar.MONTH)+1;
int day = cal.get(Calendar.DAY_OF_MONTH);
cal.add(Calendar.MINUTE, -5);
int hour = cal.get(Calendar.HOUR_OF_DAY);
int minute = cal.get(Calendar.MINUTE);
int second = cal.get(Calendar.SECOND);
          String n1= month + "/" + day + "/" +
year + " " + hour + ":" + minute + ":" + second
;
          System.out.print(n1);
        ResultSet          rs=st.executeQuery("select
count(*) from table1 where packet like '%" +
dd.substring(1,10) + "%' and time_stamp<#" +
n1 + "#");
          System.out.print("Compared string is :"+
dd);
          while(rs.next())
          {
        flag= Integer.parseInt(rs.getString(1));

//System.out.println(rs.getString(1));
          }

        }
catch(Exception e)
{
   System.out.print(e);
}
return flag;
}
```

WORKING MODEL



[5] CONCLUSION

In this research we have enhanced the security of data transmission using encryption decryption mechanism along with XOR operation. We have also used aunt colony optimization technique to restrict the transmission of packet for 5 minutes after transmission. It would reduce the chances of misuse of packet as well as it would minimize the probability of congestion in network. The used of pattern based security with AES has overcome the loopholes in existing security system. Even if craker knows the pattern he must know in which sequence button in pattern must be clicked.

References

[1] Introduction to Network Security, Dr. Rahul Banerjee, BITS-Pilani, India www.discovery.bits pilani.ac.in/rahul/CompNet/index.htm

[2] http://www.cert.org/tech tips/homeUniversitynetworks.html

[3] A Brief History of Network Security and the N d for Adherence to the Software Process Model, by Paul Innella, www.tdisecur .com/resources/assets/NetSec.pdf

[4] Network Security fundamentals, By Gert De Laet, Gert Schauwers, Cisco press.

[5]] Network Attack nd Defence, By Roger Needham and Butler Lamson. www.cl.cam.ac.uk/ rja14/Papers/SE-18.pdf

[6] Ecient countermeasures for software vulnerabilities due to memory manage-ment errors,Prof. Dr. ir. W. JOOSEN, Prof. Dr. ir. F. PIESSENS.

[7] Computer Vulnerabilities, Written by Eric Knight, C.I.S.S.P. Original Publication: March 6, 2000.www.ussrback.com/docs/papers/general/compv uln$_d$raf t.pdf

[8] http://www.antcolonies.net/howantscommunicate .html

[9] http://en.wikipedia.org/wiki/Ant colony optimization

[10] http://www.javvin.com/etrac/network-vulnerabilities.html

[11] http://searchmidmarketsecurity.techtarget.com/s Definition /0,,sid198 gci1176511,00.html

[12] A Vulnerability Assessment of the East Tennessee State University Adminis-trative Computer Network, Dr. Phillip E. Pfeiffer, IV, chair Dr. Gene Bailey Dr. Qing Yuan.

[13] http://www.infosectoday.com/Articles/Exploit Software Vulnerabilities.htm