**Security Fundamentals and Development**

**Group Report  
  
  
  
  
  
  
  
  
  
  
  
  
  
 Group 3  
 Topic 10**

**-**

**Packet Sniffing  
  
  
  
Members**

Aaron Flynn - x19404024  
Aaron O Hanlon - x19435964  
John Farrell - x19141301

Jordan Delaney - x19765711

**Due Date**

27th November

**Project Description**

Packet sniffing is a method of tapping each packet as it flows across the network; i.e., it is a

technique in which a user sniffs data belonging to other users of the network.

Aim of the Project: To have a track of the transmission of information through their network.

How does it work?

A packet sniffer is also known as a packet analyzer that contains the data that is to be

transmitted across two locations, i.e., from the sender to the intended receiver and also helps

a piece of hardware or software to monitor network traffic. Sniffers examine streams of data

packets that flow between computers on a network as well as between networked computers

and the larger Internet. This also helps in tracking and monitoring the progress of the packets

that transmit the data from the source to the destination.  
  
**Guidelines**  
Please note the following guidelines for the implementation:

* You can use any programming language of your choosing, preferably Java or Python.
* Simple GUI is highly recommended.
* You also need to submit a report of application outlining the contribution/tasks of each member of the group.
* It should at least compile & run and must include cryptography mechanisms.

**Tasks**

Research:  
    - Cryptographic algorithms and how best to implement them  
      Completed by: Everyone  
    - Packet sniffing methods:  
      Completed by: Everyone  
Tasks:  
    - Automating pinging an address the user has given (IP address or web address)  
      Completed by: Aaron O Hanlon  
    - A button that will automatically turn on wireshark for the user  
      Completed by: John + Aaron O Hanlon  
    - Implementing cryptography to encrypt and decrypt packet data  
      Completed by: Jordan  
    - GUI  
      Completed by: Aaron Flynn + John  
    - MultiThreading for windows compatibility  
      Completed by: Aaron Flynn  
    - Debugging and implementation:  
      Completed by: Everyone

**How it works**  
1. You begin the application by pressing the launch wireshark button. Once wireshark is opened and set to monitor your network, you enter the values into the text field and ping your IP address  
  
Table, Excel

Description automatically generated  
  
  
2. Once you catch the packets sent with wireshark, say by filtering by icmp, copy the data from the packet and go to the encryption window by pressing the button.  
  
Graphical user interface, application, table

Description automatically generated

3. Copy the data into input, enter a key value, and encrypt the packet data. A large string will appear in output.  
  
Graphical user interface, text, application

Description automatically generated  
  
4. Copy the output then go to the decryption window. Paste the large string into the input text area and decrypt to get the original packet data again.  
  
Graphical user interface, text, application

Description automatically generated