EasyChair Preprint

№ 1712

Tunnel comparison between Generic Routing Encapsulation (GRE) and IP Security (IPSec)

Kingsley Ogudo

October 18, 2019

Tunnel comparison between Generic Routing Encapsulation (GRE) and IP Security (IPSec)

Abstract-**The Internet growth has created a growing demand for security and privacy in the electronic communications channel. Networks have been used amongst home users, companies and organizations and most damages on the Network is due to lack of secured cyber security. If a Network is not protected or there are no measures put in place to protect the network, it will suffer from a lot of Network related attacks which will be instigated by unauthorized users (Hackers).**

Privacy and security and their important cannot be over emphasized, if internet interaction is to continue, the call for privacy and security required and has led to security body being established through policies and regulations. Internet attacks do not happen only in the form of hackers, there's computer viruses, Trojan horses, Spyware, Malware, and Computer worms that can pose a risk to internet users. These attacks come in different forms and they can jeopardize a user's privacy, which can expose sensitive information to the wrong or unauthorized user.

There's network attacks which can influence the speed of the internet for a home or office user, and there's attacks which can intercept the message sent from an authorised user to another, such as like eavesdropping. To someone who's internet savvy, internet security is of utmost importance because a lot of wrongful deeds can happen if there's no security on the network.

This paper report on the tunnel comparison between generic routing encapsulation (GRE) and internet protocol security (IPsec), and evaluate three tunnel simulation scenario and their capabilities for security and privacy measures.

Keywords: Cybercrime, Hackers, Trojan horses, malware, phishing, eavesdropping, Open System Interconnection (OSI), distributed denial-of-service, cybercrime, transmission control protocol (TCP), cyber security, internet, and internet service provider.

I. INTRODUCTION

We can talk about when was the first computer created or invented, we could talk about the abacus or inventions that followed, the slide rule, which were invented by William Oughtred in 1622. A computer invention that resembles our current computer systems was a device designed by Charles Babbage in 1871 [1].
There has been a lot of inventions after the initial invention in 1622. The first programmable unit was the Z3, which became functional in 1941, it was an invention by Konrad Zuse. Since the inception of computers, internet communication grew exponentially, leading to the development of equipment which is controlled by computers and invariably improved how communication is carried out were invented, now there's e-mail servers, database servers, file servers, backup server, and network server amongst others. [2].

Internet was a solution to the generation that was moving in an advanced setup of technology, and it would be difficult to name only one person when it comes to the creation of the internet. The internet was created by a lot of scientists, engineers, and software engineers, who came up with new features and all those features were merged to form what we know today as World Wide Web (Www) Internet [3].

Internet began to be practical in the early 1960s by J.C.R. Licklider, when the idea of computers communicating with each other was popularized. Thereafter computer developers came with the idea of packet switching, which is a method of transmitting data electronically, which became the foundation building blocks of internet, which is now commonly use in this modern world [3].

With this, cybercrime was on the increase. Crime is prevalent everywhere in the world, but ever since the introduction of internet, criminals increasingly conduct crimes on the Internet to take advantages of the less severe punishments or difficulties of being traced. In developing or developed countries, governments and industries have gradually realized the massive threats of cybercrime on the economy and public interest.
With cybercrime on the rise, cyber security needed to be implemented. The internet has no boundaries with regards to communication, so certain rules with regards to security had to be implemented and a global security body had to be established [4]

There are seven (7) layers on the Open System Interconnection (OSI) model, which a reference model for how applications communicate over a network.
The function of the OSI Model is to guide internet equipment's manufacturing vendors and software

engineers on how digital communication needs to be carried out and if correctly done, it can enable communication between different vendor equipment, and this outlines the telecommunication industry, this model is widely known as the OSI reference model.

The OSI model outlines the communication reference model layers between two networking points, it is divided into seven layers, where each layer has a function different to the preceding or the below layer. Users are on the end of these layers, even though they cannot see them physically, the only thing which a user can see is its graphic user interface (GUI).

The seven layers of the OSI Model functions on different sectors of the communication systems, which comprises of network card, networking equipment, operating systems and applications that makes it possible for signals to be transmitted over the network or other transport mediums [5].

The OSI model contains seven (7) layers in two (2) groups:

Upper layers:
7. Application
6. Presentation
5. Session

Lower layers:
4. Transport
3. Network
2. Data Link
1. Physical

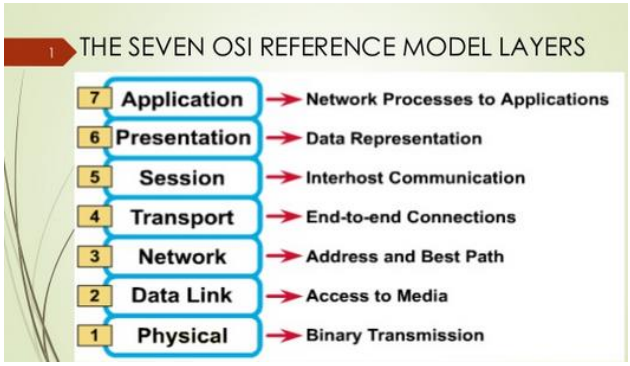

Fig 1: OSI Model

Layer 7 - Application

This is the top layer, this is the GUI. This is the layer that the user interacts with. Web browsers, and other applications that the user interacts with fall into this layer.

Layer 6 - Presentation

Presentation layer presents information for the network, this is the layer below the Application layer, it relays information to the application layer, even the network.

Layer 5 - Session

When two or more network devices communicate with each other, there's a session which is established and that is done in this layer. Setup, coordination and termination happens between applications.

Layer 4 – Transport

This layer handles the movement of data between networking end points or hosts. The size, speed, and destination of the data is handled in this layer. Most common transport protocol is the Transmission Control Protocol (TCP), which works together with the layer 3 protocol, also known as the TCP/IP suite.

Layer 3 – Network

This is the layer that handles the IP addressing of the network, this layer also handles how packets travel through the network, which is routing. Packets would not be able to traverse the network without this feature since it handles the host IP address and the destination host address.

Layer 2 – Data Link

This layer 2 handles two important sublayers which are Media Access Control (MAC) and Logical Link Control (LLC), and all the errors that are passed on from the physical layer are corrected in layer 2. It enables communication between two connected end points.

Layer 1 - Physical

At the foot of the reference model we get the Physical Layer, this layer handles the hardware and the electrical elements, that makes it possible for the network to transfer or receive data. Cable type, transmit frequency and voltage are encompassed in this layer [6].

As much as there's seven layers on the OSI reference model, in this paper our focus will be on Layer 3 security measure which is the network layer because of its internet access capabilities.

II. PROBLEMATIC

Outlined procedures that happen while in the foundation of Internet Security Association and Key Management Protocol (ISAKMP) and Internet Protocol Security while a discussion is held amongst endpoints which are in a private network

Syntax is available which can be implemented to root out faults which turn to happen on most occasions, these faults are associated with Internet Protocol Security within private network pipes, these faults can involve maximum transmission unit, network address translation, quality of service and other faults which have to do with looping.

Difficulties do happen when more than one Internet Protocol Security on a private network boundary is set in a not so correct manner. If Session passwords are described, the encrypted endpoints should understand the key that would be used when the Internet Key Exchange is negotiated.

Should private network host not have an understanding when it comes to the password that would be used, Internet Protocol Security can't begin a security association and that would cause data to flow without any protection.

A. Unsuspected Cybercriminals

Cybercrime is influenced by a lot of factors, people who commit these activities are driven by search of secret information of other users, doing what is deemed to be illegal. The below list specifies the origins of cybercrime:

1. **Government Employees:** these people know the ins and outs of how the government operates, and they have access to crucial information which can be used to their own benefit.
2. **Groups driven by financial gain:** group members here only carry out cybercrime for only one thing, which is financial gain.
3. **Staff member:** this group comprises of people who belong to a certain company and feel that whatever that was promised to them was a lie or they were misled in a certain way. These people work with sensitive information that can harm the institution.
4. **Political/Social Campaigners**: they not out there for financial gain, they there to move forward whatever they believe in, whatever that they do will obviously taint someone or a certain group in a bad light.

B. Cybersecurity Consequences and Costs

A couple of years back, a publisher in the United States, calculated the cost of hacking in that country to be in the region of over $100 billion. Other findings found that the published figure was ten times less than the actual cost of cybercrime. After 2016 the Wall Street found that the cost of cybercrime was $7.4 million, in relation to $5.9 million in 2014.

These costs will have everything included in them, like loss of income, disturbance in operation, distinguishing a type of attack, business recovery, and damage of equipment. Other than the mentioned above, cybercrime can tarnish a company's name or reputation [7].
Surprisingly, establishments that have a high level of transformation have costs that surpasses other companies. A transformation can include everything from diversity that enables the company to enter into a new market niche. Company transformation has been the major increase factor in cyberattack by 20%, this was much more compared to 18% for new features which were implemented.

Well there's no industry which is safe from cyberattacks, but most attacks are financially driven. In 2017, a data company's findings, found that 25% of undetected intrusions where to the detriment of financial institutions, hot on the heels was public sector and healthcare institutions. After 2011, financial sector was third on the rankings, after the energy sector and the utilities and defense sectors [7].

III. METHODOLOGY AND DESIGN

To investigate internet security measure, three scenario newwork was designed and simulated around the generic routing encapsulation (GRE) and internet protocol security. In Fig 2, network with IP tunneling and IPsec was designed.

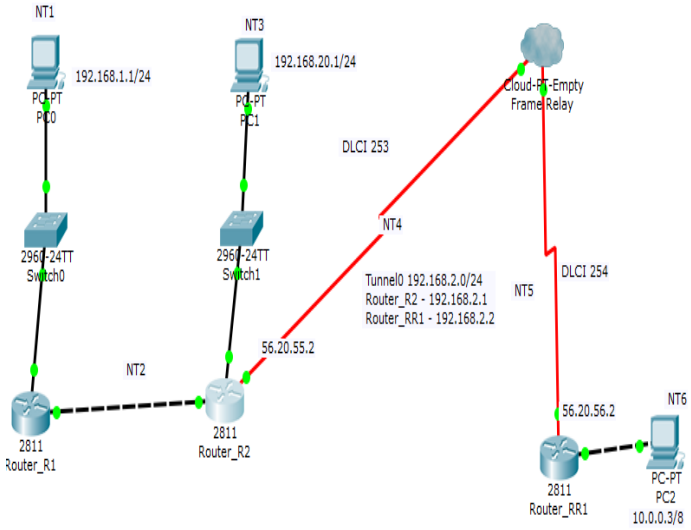

Fig 2: IP Tunneling and IPSec

Most computer users are not clued up about what happens during internet access and what is meant by network security and most importantly how their private information is protected.

The Open System Interconnection (OSI) model has seven (7) layers that characterizes and standardizes the communication functions of a telecommunication or computing system, the focus of the study will be on layer 3 of the OSI model which is the network layer, this layer is responsible for an important function in network communications which is the IP address and data routing.

To test network security on layer 3 of the OSI Model, three (3) scenarios will be created to illustrate the importance of network security. The first scenario will be a network without any security whatsoever, which will be an illustration of how vulnerable a network without security is. The second scenario will be a network with partial security, which will be an improvement when compared to the first scenario. The third scenario will be a network with full security implementation, with all the necessary security protocols. All these scenarios will show a difference in IP Headers, from an IP Header with no security to one which has maximum security.

What is positive about Internet Protocol Security is that the whole data which is related to layer 3, adding on the other upper layers are protected and vital information is not for all to see. Internet Protocol Security functions form one network layer to another network layer, the functioning part does not include the last layer of the OSI, that's why security can be implemented without the other layers having to conform to the security protocol, a widely used reason for Internet Protocol Security is to implement private networks amongst network boundaries, even between a host and remote LAN [9].

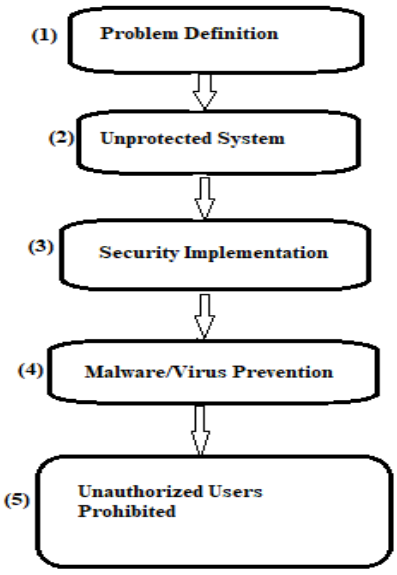

Fig 3: Predictive Study Design & Methodology

Encryption parameters were configured on both routers where tunneling was implemented, the map specifies the encryption name which is MYTEST, and the network layer security protocol which is IPSec.
For an IP Tunnel to be established, there must be a sending address and a receiving address, on the configured tunnel, the source IP address is 56.20.56.2. The peer at which the tunnel ends at is also specified at IP address 56.20.56.20.

For security measure, an IP access list 105 was configured, this security feature is used to filter unwanted data compare to the wanted ones.

A security association lifetime is also shown, this is the lifetime of the keys that the tunnel uses to encrypt data, the time and data limits are there to protect the integrity of the keys used to encrypt data, the data limit is there so that no part of the key is used twice.

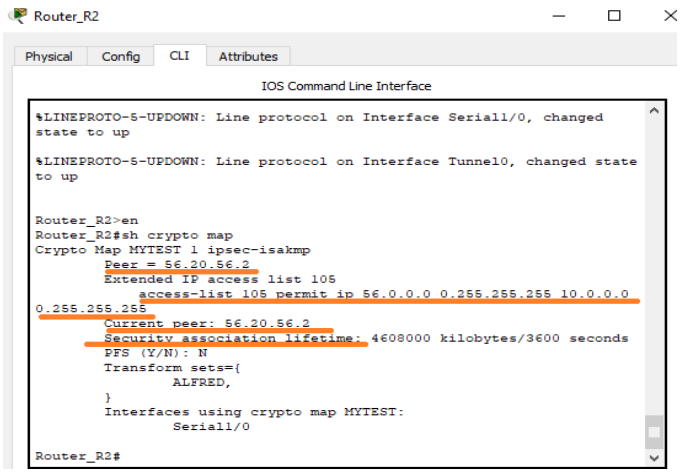

Fig 4. Confirmation of configured security map and the peer IP address.

Perfect Forward Secrecy (PFS) is set to N, PFS ensures that the same password will not be come up with twice in a row, this will push for another generation of a new key. Cyber criminals will not be able to detect what the previous key was changed into, in this case criminals would not be able to access data which has a new password, because the password which was accessed is relevant to old data, which possibly has had changes on it and would not be as useful [16].

There's a way in which a set of security features can act as security for data which is transported on the medium. While an Internet Key is being discussed, the remote endpoints need to be in one accord with what is being discussed for traffic to be passed through, this method is called transform set, and it include the below key points:

- A way for verifying the data
- A way for embedding data
- Security feature for transporting data

Set transform includes a way of verifying data, a way of embedding data, and a security feature which is used to transport data [17].

Transform sets is set to ALFRED, this is a set of protocols and algorithms specified on a gateway to secure data.

With regards to the scenarios created, scenario 1 was a network topology with no security and the packets where moving from network to network without any security. If there was to be an intrusion on the network, it would infect and destroy the operation of the network. The only protection on the network would be software-based protection, in a form of a firewall, and the protection will only protect the hosts but not the network, which would be a very risky network to be a host in.

The second scenario, which had an IP tunnel with Generic Routing Encapsulation configured on the tunnel, this scenario offered a better solution compared to the first scenario. The secret pipe used for data, the transmitting equipment embeds the data using a single routing rule, which is a rule for data, this is used on data that belongs to another node, this method is used to exchange data between the two end nodes. This scenario is better than the first scenario in a sense that there's some form of security and an IP Tunnel was created. Security will not be on the hosts alone it will also be on the routers.

The third scenario, which had an IP tunnel with IPSec configured, this scenario is better than the first and second scenario because there was a security associated configured on the routers and there was encryption and authentication configured which is better than the first and second scenario. Transform set is configured on the routers and that's a key in which peers can use to access it. Encryption Security Payload plays an important part in encrypting data that goes through the tunnel.

IV. CONTRIBUTION OF THE STUDY

Internet security is of vital importance when considering how much of the activities are performed online. This can include education, banking, communication, dating, banking and gaming.

Of all the people who use these internet applications, they would be unhappy if their private information was exposed to everyone who access the internet. There is identity theft which is used for financial gain and there's fraud which is also used for financial gain. People have been robbed millions of rand in cryptocurrency trading, all these misdemeanors has been attributed to unsecure interaction on the internet.

Internet security has been the most important feature on the internet, since the world has relied on internet to carry out most of its daily duties, a lot of wrong has happened due to tricks that have been enforced by unauthorized users.

Other countries use eavesdropping to catch and prosecute criminals, in this case the community is benefitting because dangerous individuals are removed from the society. There have been cases whereby police have

tracked a cellphone which was used during a crime, and through our current technology it would specify where it was on a certain day and time, these are exceptional cases whereby police use these methods to solve crucial criminal cases.

In contrast to these methods being used by law enforcement, hackers have also used methods like man-in-the-middle, phishing, eavesdropping, cross-site scripting, distributed denial-of-service, IP spoofing.

With the inception of internet security there has been minimal attacks on users, there are banking websites which are linked to your mobile number, once you login for internet banking there's a message that you receive on your mobile phone that needs your authentication, this verifies that the correct user is logged on.

IPSec has helped mitigate these internet attacks, with IPSec there's authentication of keys that needs to happen before communication can be open, if not, the communication will not carry on since security keys will need to synchronize on both ends. IPSec has helped when it comes to man-in-the-middle, cross-site scripting, phishing, and eavesdropping, this has reduced the number of fraudulent activities being carried out on the internet [8].

V. PROBLEM DEFINITION AND OBJECTIVES

Would it be possible to have a networking system without internet security, the answer to that would be yes, it is, but it is not recommended. To someone who is internet savvy, internet security is of utmost importance because a lot of wrongful deeds can happen if there's no security on the network.

Internet without security would be an invitation to unauthorized users with cruel intentions, internet without proper security has been exploited in the past and it has led to financial, identity, and information theft. Most internet users interact on the internet using their private and confidential information which can be exposed to hackers if the transmission medium is not protected. These below steps can be used to protect the communication medium between users:

- Static routing needs to be implemented on both gateways to avoid routing loops.
- A desired routing protocol will have to be configured on both gateways.
- An IP tunnel must be created between users (host-to-gateway or gateway-to-gateway).
- Internet Protocol Security (IPSec) must be configured on both gateways.
- Internet Security Association and Key Management (ISAKMP) must be configured on both gateways for cryptographic keys.
- A VPN tunnel will be created, which will enable both users to communicate privately on a public platform which is the internet.

VI. DATA COLLECTION

Technology has become an important tool for many non-governmental organizations (NGOs) and groups collecting data in the developing world.

A. Data Pre-processing & cleaning

Cybercriminals can instigate an attack using different methods, some to these methods can follow each other sequentially. These attacks can affect the entire network since they are able to move from one endpoint in the network to the other. This will happen only once but the damage will be through the entire network [10].

Data gathered has been from multiple Internet backbones, layer 3 interaction has made it possible for over 140 million internet addresses to be linked with unwanted internet activities around the world.

It literally says that those internet address systems which are causing mayhem on the internet, in a form of email spam, unauthorized entry to company data, distributed denial-of-service attack, cybercriminals have found a way of taking by force these systems and cause mayhem through them.

There are ways in which a security feature can enable an Internet Service Provider to track unwanted activities on the network and go as far as sourcing the Internet IP address used by these cybercriminals. If whatever criminal activity which was carried out was to an extreme extend, then the Internet Service Provider can even disable that address from causing more distraction.

These backbone providers possess a lot of data with these IP addresses that cause distraction on the network.

Unwanted internet actions have assisted in channeling or moving these addresses under the same umbrella since they have been listed and sources of malicious activities.

B. Exploratory data analysis

There's a variety of internet attacks that can expose sensitive information to hackers, these attacks are being carried out for various personal reasons, but the intention is to gain access to personal information.

C. Identifying outliers

There's challenges with regards to outliers in a network with high transmissions. Outliers might be unauthorised users, or it can present a lucrative opportunity in online trading or a dissatisfied client. On the contrary, outliers might be something which was not worth following or investigating, it can be something which is not worth your time and resources.

Spotting outliers would be the initial stage in order to find out what they all about. There are plenty of tools available to highlight if there's a sinister plan being executed, these tools are mostly in data analysis [11], [12]. Detecting outliers gets even more difficult when the data is highly variable, the surface your data sits on is not flat, or your data exists in a three-dimensional setting [11].

It was discovered that Trojan horses and Virus, Spam, Piracy and hacking are the front runners in cyber-attacks which were encountered by Internet Service Providers. This information was received by a network administrator from people who suffered these type of attacks and were under the impression that whatever data which was lost will be restored.

VII. MACHINE LEARNING ALGORITHM AND MODEL FITTING

Proper system analysis can pin point attacks quicker and deal with the attack immediately as compared to other system analysis tools. This task will be performed by a system administrator who has an idea of how attacks usually happen.

If system analysis overcomes an attack, the noble thing would be to get the ins and outs of that attack, to prepare the system for similar attacks in future. If there's a false alarm, the system needs to highlight the incident and let the daily activities to carry on as usual without any disturbance. Severe actions can be taken to mitigate that attack all to find there's nothing serious about it [14]. System analysis is used to detect abnormal activities, the main objective is to detect hacking activities and hackers on the system.

Security aspects can be divided into groups of two: The difficulties in system analysis have made it possible for attacks to be mitigated. There are other issues which where encountered but there was no viable solution to them. From a manager's point of view, the previous category has all the data which is named. With issues that didn't yield any results, there's no labeled data which can be used in mitigating or preventing cyber-attacks. The side which is not supervised is not the same as the one which is supervised. A different needs to be drawn from the supervised side and the side which is not supervised. We need to take into consideration factors like groups, reduced dimensions, rules that are related to system administration as the main objective in the not supervised analysis. The way all these scenarios will be used, will yield desired results and a better comprehension. Figure 4 below is a summary of the system analysis [15].

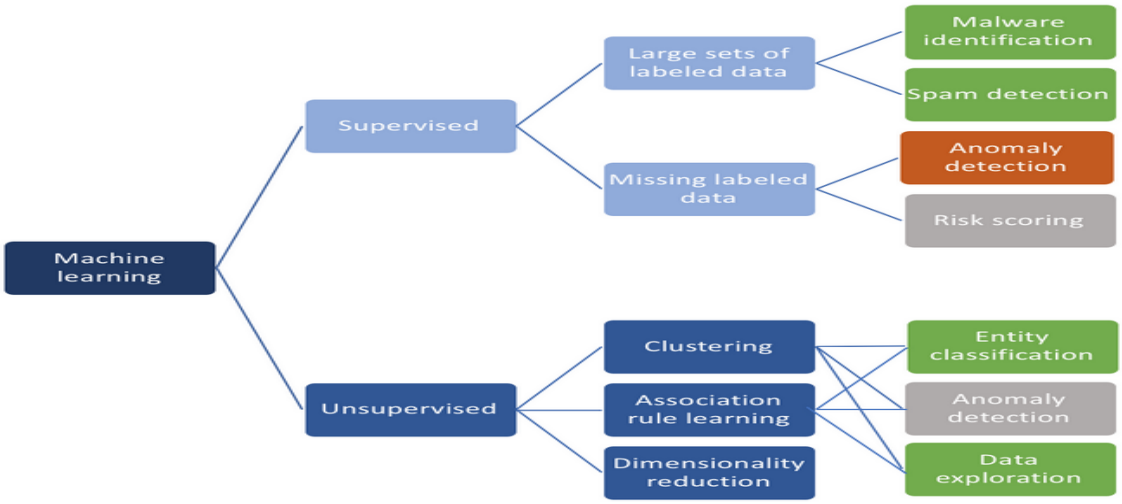

Fig 5: An incomplete view of machine learning algorithms

A. System Analysis: Supervised

System analysis has made a huge input in internet security. The above diagram is malware related, or how documents are classified, the detection of spam. The supervised side is a method of pin pointing if a file is of any use, this can be carried out without any concerns if they'll be repercussions, or if the malware will cause any damage on the system.

It is simple to identify malware in a sense that a lot of labels are used. These representatives give way in which security can be learned deeper and how a network would behave or react in such circumstances. The challenge in identifying spam is the same because there's a lot of information which can be used to guide the system in terms of what's wanted and what's not.

B. System Analysis: Not Supervised

On the unsupervised side, let's start with dimensionality reduction. Applying it to security data works well, but again, it doesn't really bring us any closer to finding anomalies in our data set. The same is true for association rules. They help us group data records, such as network traffic.
A group of features could help in resolving the abnormal activities. It has been revealed that the main issue with grouping in security are the ways in which certain rules are implemented, how to relate the co-operation of these features.

C. Knowledge and context

The above set of rules can be used as mechanism in sensing possible attacks, if they are correctly used. Factors can be any information which assists in comprehending the roles that the features play in information analysis, it might be user related or machine related. Factors for equipment might involve the role which is played, where it's situated, who have rights to it, and so on.

Instead of inspecting network data separately, we must include added information, so the inspection of data can be useful. All the necessary questions that we have, the system will be able to come up with answers or solutions. If we know the functions of every device in the network, if there's a strange behavior from that device then we know that somehow an attack was initiated.

Knowledge is key, if a system is built with the knowledge of what needs to happen when and where, then half of the problem is sorted. Systems which can assist in pin pointing the weakest link are necessary, it could be helpful if the systems don't offer a solution immediately but can offer more information to security administrators, so they can plan forward with regards to such attacks.

VIII. CONCLUSION

There's plenty of cybercrimes on the internet and IPSec and GRE wouldn't be enough to combat the spread of cybercrimes. A lot must be implement before and after the tunnel for cyber security to be tight.

With ISPs being responsible for internet services, in most cases they do pick up if there's a sinister activity being carried out on the internet service provided, and the person's IP address and port number can be blocked.

With regards to Supervised and Unsupervised algorithms, with a supervised algorithm, it is easier to pick up malware and spam, which can assist in reducing the number of infections and unauthorized user access to private and confidential information. Unsupervised algorithm is usually not the ideal scenario since data exploration, entity classification, and anomaly detection happen at an advanced stage.

LARIAT's model expands the supervised algorithm in a sense that it provides tools to assist evaluation and configuration for information assurance systems. Another aspect which is covered is false alarms, which can waste time and resources in uncovering the integrity of the alarm. The model has the ability of pinpointing the type of attack, the victim's IP address and port number, the scripts, and what does the attack require. Internet security can be implemented in various methods, and LARIAT's model has proved that a lot must be implemented before and after the IP tunnel for security to be tight.

Generic Routing Encapsulation offers minimal network security, it's a tunneling protocol that can encapsulate a wide variety of network layer protocols inside a virtual point-to-point link over the Internet, there are other features which are necessary for a packet to be protected in transit to its destination. With attacks such as man-in-the-middle, it would be much easier for a hacker to gain access to the network, even eavesdropping will be easier to carry out since there's no encryption and authentication on the packet. GRE's advantage is that it's used by IP tunneling to expand networks across a single-protocol backbone environment by connecting multi-protocol subnetworks.

IPSec has more advanced security features, it has cryptographic security services which are important in securing a packet. Cryptographic service provides software-based encryption and decryption services. It contains implementations of cryptographic standards and algorithms.

IPsec also uses Internet Key Exchange to unsure security for virtual private network negotiation and remote host or access. IKE defines an automatic means of negotiation and authentication for IPSec security associations.

IPSec also verifies if a packet has been unaltered in a form of Secure Hash Algorithm, this is done by producing a checksum before the file has been transmitted, and the again once it reaches its destination.

Hash Message Authentication Code (HMAC) is also used by IPSec as a specific type of message authentication code involving a cryptographic hash function and a secret cryptographic key.

Triple Data Encryption Algorithm (3DES) is used by IPSec as a symmetric-key block cipher which applies the Data Encryption Algorithm three times to each block of data. IPSec uses an Encapsulation Security Payload (ESP) for providing authentication, integrity and confidentiality of packets, data/payload in IPv4 and IPv6 networks.

With all the features that IPSec offers it's clear that IPSec offers a better packet security because Generic Routing Encapsulation only encapsulates a packet without any form of security. Cyber-attacks like man-in-the-middle, phishing, eavesdropping and DDoS will be hard to implement on a network which uses IPSec, but if a network uses GRE it will be a walk in the park for hackers to instigate attacks on the network. In conclusion, IPSec with all its features provides a better security option compared to GRE.

IX. FUTURE STUDIES

As cyber-attacks continue to skyrocket, and criminals use increasingly complex methods, so those trying to prevent these attacks need to equip themselves with the tools to do so. This means staying on the cutting edge of information technology and IT skills development. Detecting unauthorized users is one of the most important skills, it can mean that attacks can be stopped even before they are carried out, these types of attacks play a huge role in cyber-attacks and more people need to equip themselves with such skills.

Internet security and overcoming the risks associated with it, more people should be technology savvy, this will assist in recognizing if a system has a problem or not.

Another aspect which I feel needs to implement with regards to Internet security is to implement a security protocol which will function on layer 4 of the OSI model but it should work together with security features of layer 3. As much as these layers have different functions, I feel that there should be a protocol which is implemented that can feed layer 4 with security information, since layer 4 handles the transportation of data, that type of security protocol will be more effective in a sense that even though these layers have different functions but can co-operate with the security information.

X. REFERENCES

[1] Who invented the computer? By William Harris, HowStuffWorks.

[2] How to Make Zuse's Z3 a Universal Computer, by Raul Rojas, September 5, 1997.

[3] Who invented the internet? By Evan Andrews, December 18, 2013.

[4] Guillaume Lovet Fortinet, Fighting Cybercrime: Technical, Juridical and Ethical Challenges, VIRUS BULLETIN CONFERENCE, 2009.

[5] Network Design & IT Standards and organizations, by Margaret Rouse, Daniel Kroon and Kara Gattine.

[6] The OSI model explained: How to understand the 7-layer network model, by Kieth Shaw, December 4, 2017.

[7] Cybersecurity: What Every CEO and CFO should know by, Melisa LIN

[8] Advantages and Disadvantages of IPSec, Best Reviews

[9] Network Security – Network Layer, tutorials point simply easy learning

[10] Analysis of Network Attack and Defense Strategies by Y.Sun, W. Xiong, K. Moniz, & A. Zahir, pg 5 – 7

[11] Big Data Outlier Detection, for Fun and Profit, by Alex Woodie, September 30, 2014

[12] A Brief Overview of Outlier Detection Techniques, by Sergio Santoyo, September 11, 2017

[13] Here's another reason to think twice before using your debit card, by Kelli B. Grant, March 6, 2018

[14] Machine Learning and Endpoint Protection – Separating Hype From Value, Palo Alto Networks Inc.

[15] AI and Machine Learning in Cyber Security, by Raffael Marty, June 2016.

[16] Handbook of Applied Cryptography, by Alfred Menzies, Paul C. van Oorscot, Scott Vanstone, 1997.

[17] Cisco Secure Virtual Private Networks, Cisco Press, by Andrew Mason, December 18, 2001