International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:3, 2016

Enhancing the Network Security with Gray Code

Thomas Adi Purnomo Sidhi

***Abstract*—**Nowadays, network is an essential need in almost every part of human daily activities. People now can seamlessly connect to others through the Internet. With advanced technology, our personal data now can be more easily accessed. One of many components we are concerned for delivering the best network is a security issue. This paper is proposing a method that provides more options for security. This research aims to improve network security by focusing on the physical layer which is the first layer of the OSI model. The layer consists of the basic networking hardware transmission technologies of a network. With the use of observation method, the research produces a schematic design for enhancing the network security through the gray code converter.

***Keywords*—**Network, network security, gray code, physical layer.

I. Introduction

AS we know, one of the aspects in delivering a good network capability is security. Some researches have been done to enhance and to refine methods to improve network security. In this paper, a way to enhance the network security is proposed. The research is based on the need to enhance our network security and our concern focuses on networking breach in bandwidth theft. As computer networks become more heterogeneous, applications must increasingly deal with suboptimal network conditions [1].

This research started to solve the problem when a network enterprises provided cloud computing in order to cut down cost and increase profitability [2]. Even in small enterprises, successful implementation of cloud computing requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures [3]. One way to solve these problems is proposed in this paper.

Young Jin Jung states that all optical signal processing has attracted scientists' attention for a long time and various all optical *Boolean* logic gates have been implemented [4]. However, it has not yet been implemented on network physical layer. Jung has proven that building Gray code to the binary coded decimal converter is possible. This paper proposes a new design to build a repeater that functions to convert binary to gray code, and vice versa. With this conversion, automatically, all cables that go through the building exterior can be secured, because when any person tries to steal the bandwidth through the cable, the conversion will process the transmission that is still in binary, and the stolen data will be invalid. The connection being captured or taped will need to be decoded before being read.

Thomas Adi Purnomo Sidhi is with the Informatics Engineering , University of Atma Jaya Yogyakarta, Jl. Babarsari 43, Yogyakarta 55281, Indonesia(e-mail: th.adi.ps@staff.uajy.ac.id).

II. Literature Review

A. Basic of Networking

A computer network consists of a collection of computers, printers and other equipment connected together so that they can communicate with each other. Broadly speaking, there are two types of network configuration, peer-to-peer and client/server networks.

Peer-to-peer networks are more commonly implemented where less than ten computers are involved and strict security is not necessary. All computers have the same status, hence the term is 'peer', and they communicate with each other on an equal footing. Files, such as word processing or spreadsheet documents, can be shared across the network and all the computers on the network can share devices, such as printers or scanners, which connect to any one computer. Client/server networks, on the other hand, are more suitable for larger networks. A central computer, or 'server', acts as the storage location for files and applications shared on the network. Usually the server is a higher than average performance computer. The server also controls the network access of the other computers, which are referred to as the 'client' computers. Typically, teachers and students in a school will use the client computers for their work and only the network administrator (usually a designated staff member) will have access rights to the server [5].

In this paper, we also use OSI Model, The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO).

The model groups similar communication functions into one of seven logical layers. This layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communication across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connecting on that layer.

Layer 1: Physical Layer

The physical layer has the following major functions:

- It defines the electrical and physical specifications of the data connection. It defines the relationship between a device and a physical transmission medium (e.g. a copper or fiber optical cable). This includes the layout of pins, voltages, line impedance, cable specifications, signal timing, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.

- It defines the protocol to establish and terminate a connection between two directly connected nodes over a communications medium.
- It may define the protocol for flow control.
- It defines a protocol for the provision of a (not necessarily reliable) connection between two directly connected nodes, and the Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over the physical communications channel. This channel can involve physical cabling (such as copper and optical fiber) or a wireless radio link.

The physical layer of Parallel SCSI operates in this layer, as do the physical layers of Ethernet and other local-area networks, such as token ring, FDDI, ITU-T G.hn, and IEEE 802.11, as well as personal area networks such as Bluetooth and IEEE 802.15.4.

Layer 2: Data Link Layer

The data link layer provides a reliable link between two directly connected nodes, by detecting and possibly correcting errors that may occur in the physical layer. Point-to-Point Protocol (PPP) is an example of a data link layer in the TCP/IP protocol stack. The ITU-T G.hn standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer which provides both error correction and flow control by means of a selective repeat Sliding Window Protocol.

Layer 3: Network Layer

The network layer provides the functional and procedural means of transferring variable length data sequences (called datagrams) from one node to another connected to the same network. A network is a medium to which many nodes can be connected, on which every node has an address and which permits nodes connected to it to transfer messages to other nodes connected to it by merely providing the content of a message and the address of the destination node and letting the network find the way to deliver ("route") the message to the destination node. In addition to message routing, the network may (or may not) implement message delivery by splitting the message into several fragments, delivering each fragment by a separate route and reassembling the fragments, report delivery errors, etc.

Layer 4: Transport Layer

The transport layer provides the reliable sending of data packets between nodes (with addresses) located on a network, providing reliable data transfer services to the upper layers. An example of a transport layer protocol in the standard Internet protocol stack is TCP, usually built on top of the IP protocol.

Layer 5: Session Layer

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

Layer 6: Presentation Layer

The presentation layer establishes context between an application-layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation layer data units are encapsulated into session protocol data units, and passed down the stack. This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer. The original presentation structure used the Basic Encoding Rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.

Layer 7: Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network or the requested communication exists. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

B. Network Security

Deployment of an effective and scalable network security system requires proper designing according to risk analysis results as well as security principles. Network safeguards are the first protection barrier of IT system resources against threats originating from outside the network (e.g., intruders, malicious code) [6].

Network security is now concerned not only with preventing external attacks, but also the internal ones too. Securing the network from external intruders will mitigate only a percentage of internal risk [7].

Protection of IT system resources is based on many security layers as shown in Fig. 1. Extensions of the defense-indepth principle are the following rules [6]:

- Layered protections – security layers complement one another: what one misses, the other catches.
- Defense in multiple places – security defenses are located in different places on the IT system
- Defense through the diversification – safety of IT system resources should be based on the protection layers consisting of different types of safeguards. When two layers of the same type are being used (e.g., two network firewalls), they should come from different vendors. This rule should be used cautiously as it increases the complexity of the security system and can complicate and increase the cost of management and maintenance.

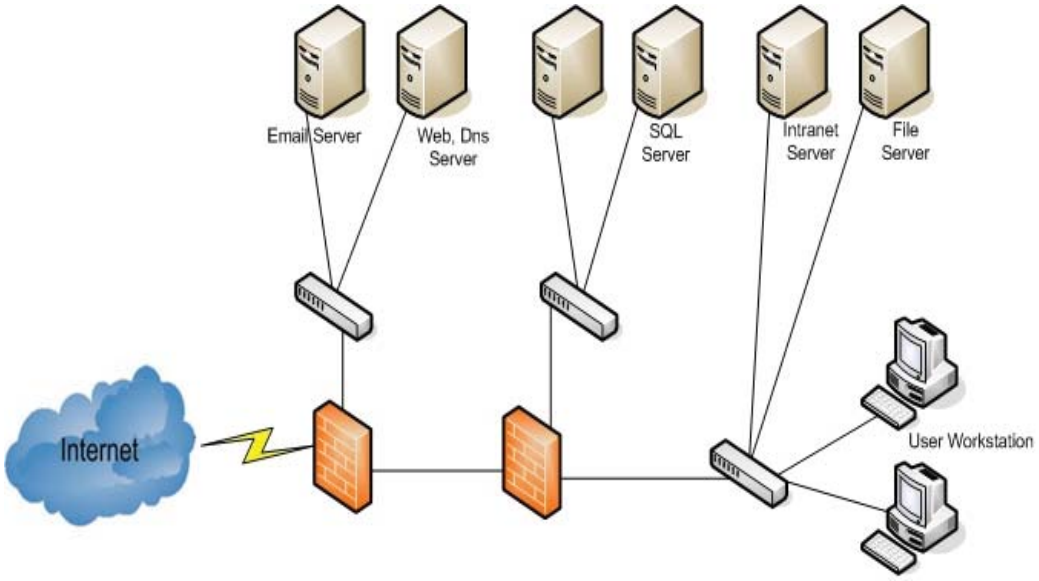

Fig. 1 Defense-in-Depth principle [6]

C. Network Thread

Many different types of Network threats exist, but many threats fall into three basic categories [8]:

- Unauthorized access: Unauthorized access is when an unauthorized entity gains access to an asset and has the possibility to tamper with that asset. Gaining access is usually the result of intercepting some information in transit over an insecure channel or exploiting an inherent weakness in a technology or a product. Getting access to corporate network resources is usually accomplished by doing some reconnaissance work. Most likely, the corporate network will be accessed through the Internet, tapping into the physical wire, remote modem dial-in access, or wireless network access.
- Impersonation: Impersonation is closely related to unauthorized access. Impersonation is the ability to present credentials as if you are something or someone you are not. These attacks can take several forms: stealing a private key or recording an authorization sequence to replay at a later time. These attacks are commonly referred to as man-in-the-middle attacks, where an intruder is able to intercept traffic and can, as a result, hijack an existing session, alter the transmitted data, or inject bogus traffic into the network. In large corporate networks, impersonation can be devastating because it bypasses the trust relationships created for structured authorized access
- Denial of service (DoS): is an interruption of service, either because the system is destroyed or because it is temporarily unavailable. Examples include destroying a computer's hard disk, severing the physical infrastructure, and using up all available memory on a resource.

There is so much explanation of network threat to learn, but with this research, we are concerned with the Physical Wire security that usually threatens by taping it with another device. The ease or difficulty of packet snooping (also known as eavesdropping) on networks depends largely on the technology implemented. Shared media networks are particularly susceptible to eavesdropping because this type of network transmits packets everywhere along the network as they travel from the origin to the final destination. When concentrators or hubs are used in a shared media environment (such as FDDI, 10BASE-T, or 100-Mbps Ethernet), it can be fairly easy to insert a new node with packet-capturing capability and then snoop the traffic on the network. As shown in Fig. 1, an intruder can tap into an Ethernet switch and, by using a packet decoding program such as EtherPeek or TCPDump, read the data crossing the Ethernet.

D. Gray Code

Absolute encoders provide parallel absolute position information in a binary format. Some absolute encoders use a special binary code known as gray code. The main characteristic of gray code is that only one bit differs from any adjacent numbers [9].

Converting Gray Code to Binary Code [9]:

This method converts gray code to natural binary. At each step, an example shows the conversion process for the decimal value 141.

STEP 1. Begin with the highest order gray code logical "one" in the Gray code. The corresponding bit in the natural binary word will also be a logical "one".

Example:

Decimal	Gray Code	Intermediate Binary
141	11001011	1 - - - - - - -

STEP 2. Complement the next digit in the Gray Code word to obtain the corresponding digit for the equivalent binary word.

Example:

Decimal	Gray Code	Intermediate Binary
141	11001011	10 - - - - - -

STEP 3. If the binary digit obtained in the previous step is a logic "zero", the following binary digit will be the same as its corresponding Gray code digit. If the binary digit is a logical "one" the following binary digit will be the complement of its corresponding Gray code digit.

Example:

Decimal	Gray Code	Intermediate Binary
141	11001011	100 - - - - -

STEP 4. Repeat Step 3 for each successive lower order digit.

FINAL RESULT:

Decimal	Gray Code	Intermediate Binary
141	11001011	1000 - - - -
	10001 - - -	
	100011 - -	
	1000110 -	
	10001101 Binary Value	

Converting Binary Code to Gray Code:

STEP 1. Start from the least significant bit of the natural binary. The corresponding gray code bit will be the same if the next significant digit in the binary word is a logical "zero". The Gray code digit will be the complement of the corresponding natural binary bit if the next significant digit in the natural binary is a logical "one".

FINAL RESULT:

Decimal	Natural Binary	Intermediate Code
141	10001101	- - - - - - - 1
		- - - - - 011
		- - - - 1011
		- - - 01011
		- - 001011
		- 1001011
		11001011 Gray Code

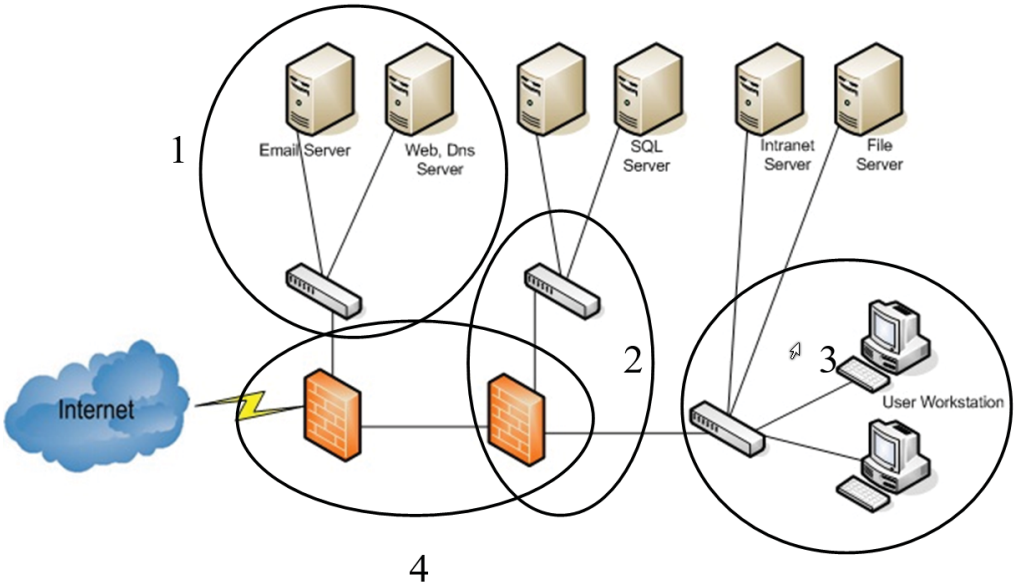

Fig. 2 Defense-in-Depth principle [5]

III. Research Methods and Result

The method that we use for this research are "observation" on the "local network security" and experimental trial and error. According to Defense-in-Depth principle, there are 4 types of internal connection as shown in Fig. 2.

The 4 types of internal connection shown on Fig. 2 are the connection from:

1. Server and Switch
2. Switch and Firewall
3. Switch and User Workstation

4. Firewall and Firewall

The enhancement can be done by adding the converter to gray code "adapter" from the binary that is used for transports data. This enhancement is functioning like a repeater, it enhances the signal and offcourse it's convert the signal that transferred in the physical layer to gray code. Every edge of the connection (end of the cable connector) is connected to a gray code converter before being attached to the device. This scheme can be seen in Fig. 3.

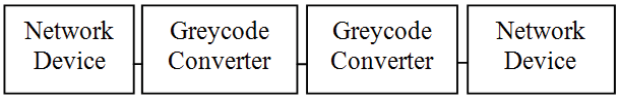

Fig. 3 Gray code converter placement

The connection from the device through converter are supposed to be in the same room where the device is located. The connection through converter will be split and converted every 4 bit, to gray code, and the result will be sent serially without any delay. On the other end, the connection will be caught by the gray code converter to be converted again to binary.

IV. Conclusion

In this paper, the author proposes the idea to enhance network security through a gray code converter used in every edge of the connection in the internal network. This method can be used optionally not just by the gray code converter, but also another scheme of encryption and decryption. The enhancement can prevent a network breach such as phishing, but only on the physical layer and on the internal network. This enhances security can also protect the resource that goes through the cable, so the bandwidth stealing can be minimized. Another way to use this scheme is through a WiFi modem, this scheme can also privatize the hotspot because it will need a specific modem to access it.

For future use, this idea can be included with switch or hub construction, with the option of data transferring via toggle for changing how format data will be sent through the cable.

References

[1] J. Li, M. Yarvis, P. Reiher, "Securing Distributed Adaptation,"in Computer Networks, University of California, Los Angeles, CA 90095, USA

[2] Brandl D.,"Don't cloud your compliance data," in Control Engineering, page 57, January, 2010.

[3] S. Saidhbimca and I. Gashaw, Security Concerns in Medium Size Enterprise Cloud Computing, IJARCET, Volume 2, Issue 8, August 2013.

[4] Y. J. Jung, S. Lee, N. Park, "All-optical 4-bit Gray code to binary coded decimal converter", in Optical Components and Materials V, Proc. of SPIE Vol. 6890 68900S-1, 2008.

[5] T. Bakardjieva, "Introduction to Computer Networking", Institute of Technology, Varna Free University "Chernorizec Hrabar".

[6] Mariusz S, "The Principles of Network Security Design," in ISSA Journal, October 2007, pp. 29-31.

[7] Check Point, Security Architecture, Chapter 9 Page 157-176, Downloaded 13 December 2013.

[8] Cisco, "Threats in an Enterprise Network", in Designing Network Security, 2nd Edition, Chapter 5, Cisco System, Inc., 2005.

[9] Application Note #5412, Galil Motion Control, Inc., 3750 Atherton Road Rocklin, CA 95765 USA www.galilmc.com.