A Novel Security Approach for Access Model

Teena Jaiswal
Department of Computer Science, Makhanlal Chaturvedi National University. BHOPAL (M.P)

Umesh Kumar Singh
School of Engineering & Technology, Vikram University, Ujjain(MP)

Shabana Sheikh
Department of computer Application, Govt. Girls PG College, Ujjain (MP)

ABSTRACT
In vision of the importance of researcher's sharing the same theory of network security, this paper suggests a novel security approach for network security in which network security issues can be treated essentially. The meaning of network security has been identified for some time, but provides networks (especially public networks) with security utilities has proven difficult. The act of the network itself in computer network security has been minimum , as systems certainly preserve their own security. To resolve such problems, this paper recommends a network security approach for the access model.

Keywords
Access policy, network security, VPN, Close User Group, Wireless sensor network.

1. INTRODUCTION
A network is considered as a wired or wireless network, if the access medium is some kind of physical cable connection between the workstations, such as a copper cable or a fiber-optic cable. Alternatively, a network is considered as a wireless network if the access medium depend on some kind of waving through the air, such as radio frequency (RF) communication. A network can also be distributed according to its geographical coverage. Depending on its size, a network can be a personal area network (PAN), a local area network (LAN), a metropolitan area network (MAN), or a wide area network (WAN).[6] The progress of the information society has carried with it a natural demand to make communications systems more open. However, performance this risk exposing systems to the vulnerability of illegal access .Systems should become available to strange users who are not regular members of a system's user group. Such users may access systems from remote sites via communication networks. To manage with new situations like these, strong security mechanisms will be required in every wired and wireless system. Furthermore, additional security roles in the networks themselves will be necessary .While the significance of network security has been accepted for some time, providing networks (especially public networks) with security utilities has verified difficult .The role of the network itself in computer network security has been minimal, as computers certainly preserve their own security. In observation of the importance of researchers sharing the same idea of network security, this paper proposes a novel approach to the reference model for network security in which network security concern scan be treated essentially.

2. SECURITY ISSUES IN NETWORKING
Security issues in wired and wireless networks (especially public networks), the tapping of telephone wires has been discussed and many techniques for hiding information have been proposed. Several ways of prevent illegal access to the system have been discussed such as using ID cards or passwords when entering machine rooms and using console keyboards. As most network traffic based traditionally consisted of voice communications, network security issues other than those mention over have rarely been discuss .As a outcome of latest enhance in non-voice traffic which have mirrored the development of today's information society, the importance of network security has now been recognized. It is much more difficult to identify the receiving terminal in non-voice telecommunication services than it is in man to man voice transmission .Moreover, as network shave become more complex and as their level of functioning has increased, databases have been introduced to control service is and manage the networks themselves. A new threat from the point of view of security is the illegal accessing of such databases. Other threats are illegal leaks of important secret information as a result of complex network use such as resource common use in VPNs (virtual private networks) and connections between public network sand leased lines (or private networks). The social importance of networks has improved and providing networks (especially public networks) with their individual security purposes has become a necessary issue. In [7], a secure network access system is presented. It provides node authentication, packet authentication, packet integrity, packet confidentiality.

3. CURRENT STATUS OF NETWORK SECURITY
Network security surveys other than those concerned with monitoring and the illegal accessing of systems have been done essentially in the computer network field. There, as the information society has developed, security in computer networks has been discussed as an essential issue. [5]

3.1 Computer Networks
In computer systems in which a large amount of information is stored and processed, illegal leaks and the illegal alteration of information are big problems. Therefore, in the computer field, security issues such as security models and access models have been studied from the early stages, and several technical solutions for security problems related to encryption and authentication have been proposed. Examples of security models being studied include the Bell and La-Paula model [11, Take-Grant model [2], Clark-Wilson model [3] and Chinese Wall model[4].In access control design, which aims to prevent illegal access rules between the object, being accessed and the subject doing the accessing, are described and the access from subject to object is controlled by following the described rules. The principle of these rules is called "security policy" .The system in which computers are connected via a network is called a computer network. Investigations into computer network security are being focused on illegal access to computers via networks. However, in the discussion on computer network security, the role of networks as seen from the point of view of security is virtually nil. It is the computer terminals, which are equipped

with concrete security functions that ultimately maintain security. Network design is a well-developed procedure that is based on the Open Systems Interface (OSI) model. The OSI model has many advantages when design networks. This also defines seven layer of security Model and offers modularity, flexibility, ease-of-use, and consistency of protocols. The protocols of different layers can be easily shared to generate stacks which permit modular expansion. The performance of individual layers can be changed later with no creation other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed practice. There isn't a methodology to control the complexity of security requirements. Secure network design does not enclose the same advantages as network design. Bio metrics provides a well method of verification than passwords. This reduces the illegal access of secure systems. New technology such as the smart card is growing in research on network security. The software feature of network security is very active.

3.2 Hardware and Software Developments

Hardware growths are not evolving quickly. Smart cards and Biometric systems are the individual new hardware tools that are broadly impacting security. The cost of hardware devices is one object that may lead to the well-known employ of voice biometric security identification, especially between corporations and organizations on a low budget. Hardware equipment such as computer mice with built in thumb print readers would be the next boost. These devices would be more expensive to employ on several work station, as each machine would require its own hardware device. The benefit of voice recognition software is that it can be central, thus reducing the cost of performance per machine. Obviously, someone can easily steal a smart card from someone else .The smart card is cost-effective but not as secure as the biometric identification devices.

The software phase of network security is very huge. It includes firewalls, antivirus and IDS. The research development of all security software is not possible to study at this point. The goal is to achieve a view of where the security software is caption based on emphasis being placed now. The extension of the standard security software still remains the equivalent. When new viruses come into view, the antivirus is updated to be able to observe beside those threats. This procedure is the similar for firewalls and IDS systems. a lot of research papers that have been skimmed were based on examine attack pattern in order to create smarter security software. As the security hardware transitions to biometrics, the software also desires to be able to use the information correctly. Recent research is being performed on security software with neural networks. The objective of the research is to use neural networks for the facial detection software. Many small and difficult devices can be connected to the internet. Most of the current security algorithms are computational rigorous and require significant processing power. This power, however, is not accessible in tiny devices like sensors. Therefore, there is a need for designing light-weight security algorithms. Research in this area is currently being performed.

3.3 Network Security

In network security, it must be highlighted that the entire network is protected. Network security does not only concern the security in the computers at every end of the communication sequence. When spreading data the communication channel should not be vulnerable to attack. A probable hacker could target the communication channel, get the data, and decrypt it and re-insert an incorrect message. Securing the network is just as considerable as securing the Pc's and encrypting the message. When creating a secure network, the following security services to be measured.

1. Access — permitted users are provide the means to Communicate to and from an exact Network.
2. Confidentiality – Information in the network remains private
3. Authentication – Certify the users of the network are who they say they are
4. Integrity – Certify the message has not been improved in transit
5. Non-repudiation – Ensure the user does not contest that he used the network An real network security plan is developed with the understanding of security issues, possible attackers, required level of security, and factor that make a network vulnerable to attack.[8]

Studies into security harms of networks themselves (especially public networks) have just started. Most of these studies are relying to some extent on the results of studies into computer network security. Thus, studies into overall network security which aim to provide a common conceptual accepting of the problem are not presently being done. With respects to network models from the point of view of security, some models have been proposed, but no compromise has yet been extended .In addition to researching network security, developing a mutual awareness of the conception of network security, learning how to handle the issues related to this topic and exploratory policies aimed at resolving them will all play an essential role in the progression of that research. Therefore, a model that can both integrate the several problems of network security and permit them to be understood hierarchically is required.

4. NETWORK SECURITY MODELS

4.1 Model Design Characteristics

1. Straight models

Computer networks-

In most computer network models; the network itself provides denial security within the computer network-only computer have security functions. Thus, it can be said that there are no schemes for security models for networks.

Network design models

Although many studies have been conducted into network design models in current Intelligent Network research, the partition of networks into a communication plane and a service plane has been completed from the point of view of service execution. Therefore, these studies have not explained network security problems.

Models of networks with essential security-

Existing models of networks with essential security have addressed specific problems, rather than assist as concept models. Therefore, no shared accepting of overall security problems has been developed that can pact with a wide range of network security concerns. Basic structure of model .The model contains of five layers from the point of view of network configuration components.

2 Proposed models

Basic frame of model-

The model consists of five layers from the point of view of network configuration elements.

Considerations in model design

from the point of view of clarifying subjects to be considered, the following points are considered.

- The model's structural elements must be clear.
- The subjects must readily correspond to the actual issues.

From the point of view of achieving common awareness, the following points regarding a common understanding are considered.

- Definitions must be simple.
- All targeted issues must be present.

4.2 Model

1 Vertical structure of Reference model:-

The network elements which, from the point of view of security, may be accessed illegally are classified hierarchically and security issues in each layer are studied integrally. A network can generally be thought of as a collection of individual networks. An individual network consists of switching systems, transmission systems, and telecommunication processing systems and so on. Data may be present in all of the various telecommunications equipment. Thus, vertically, five layers are considered: WSN, inter networking, individual networks, telecommunications equipment and data (See Fig1).

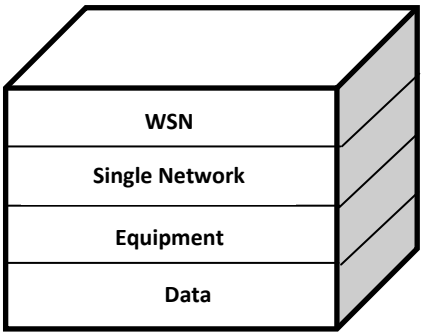

fig1, Proposed Network Security Model

WSN-

As shown in fig2 This level addresses security items related to access between networks. Individual networks are physically or logically independent. When a CUG (Closed User Group) service is considered, each CUG is treated as a single network. A WSN is large number of sensors distributed over a sensor field using one or more base stations. In this case, all sensor nodes trust the base station. Base station serves as access point for network administrator and management of security services. Sensor nodes are the access points for user (laptop, mobile phone) to data in the WSN. Only authorized users have to access the WSN's data .The security of paths and data in the network is the main matter for discussion here, as shown in Fig3.

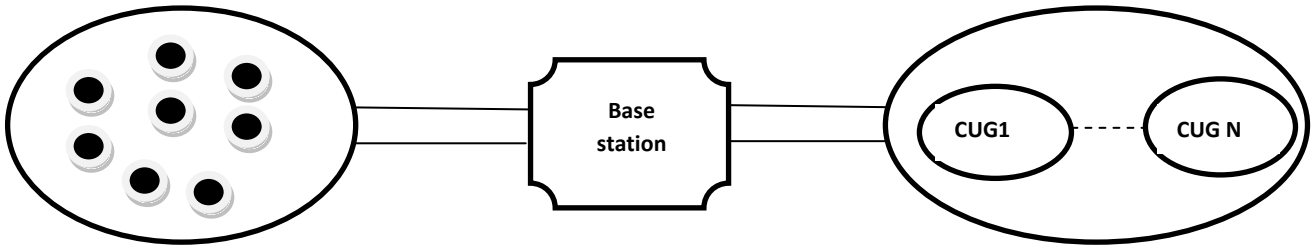

Figure 2:- Wireless network

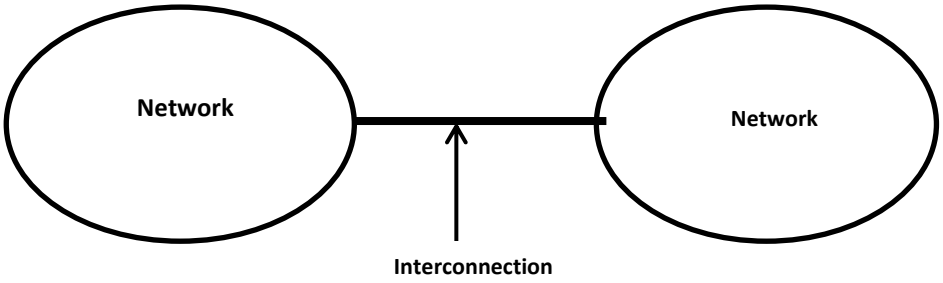

Figure 3:-Internetworks

This level does not give any significance to the configuration of terminals, even if a terminal consists of LAN or WAN. Therefore, this level does not treat terminal problems as internetwork ones. In the case
where problems are treated as internetwork matters, terminals are defined as a networks and the problems of inter networks are then investigated.

Single networks-

This level addresses security items related to accessing individual networks. The security of paths in the network

is the main matter for discussion here, as shown in Figure 4.

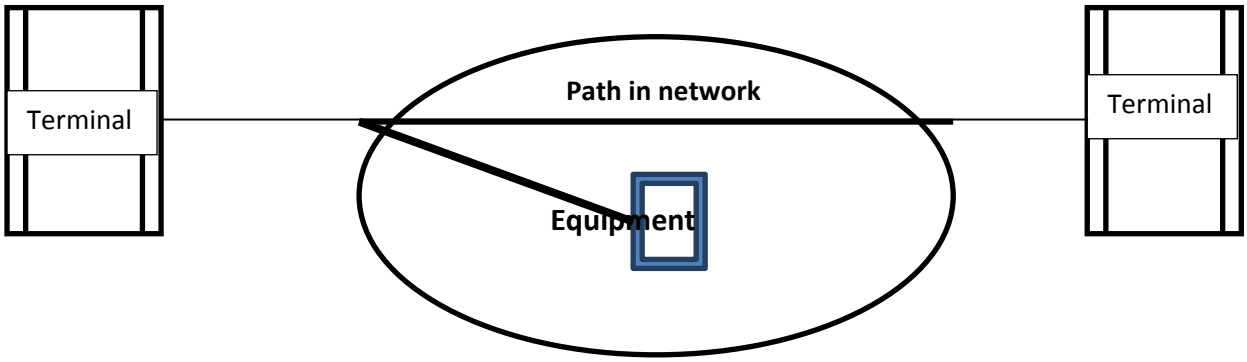

Fig 4 Single network

Telecommunications equipment-

As shown in Figure 5, this level addresses accessing the telecommunications equipment that make up an individual network. At this level, simple access control and the problem of congested equipment caused by so-called improper access are handled. Wiretapping and the illegal accessing of the system by intruders are treated in this layer. However, as access is not made via networks in these cases, but rather directly at the objects themselves, it is better to discuss these problems in adifferent category.

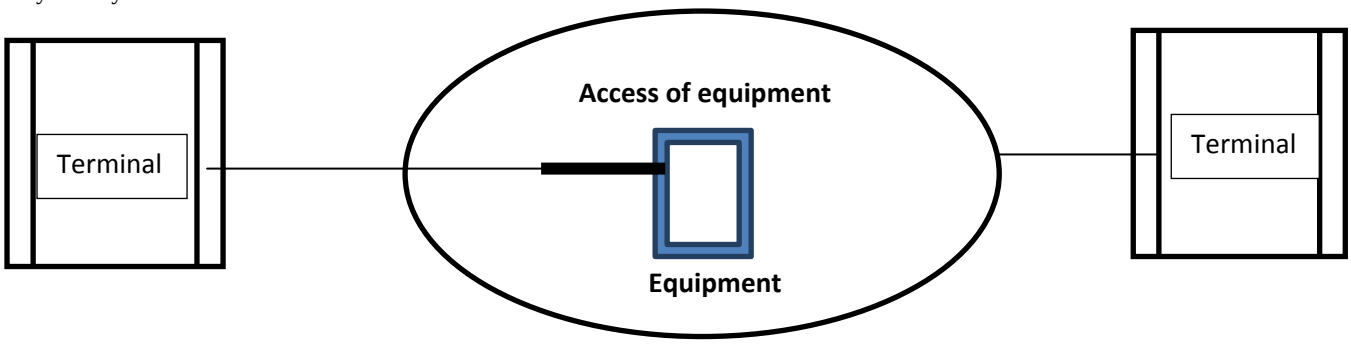

Fig 5-Telecommunicationsequipment

Data (positive/passive) –

This level addresses security items related to accessing data stored inside telecommunications equipment as shown in Figure 6. Data are programs and resident data, the former being called positive and the latter passive.

To prevent illegal access to positive data, other than in the cases of data modification and leaks, illegal execution should be prevented. Moreover, in consideration of the fact that user programs will be loaded into network equipment in the future, the effects of the user program's bugs should be taken into consideration.

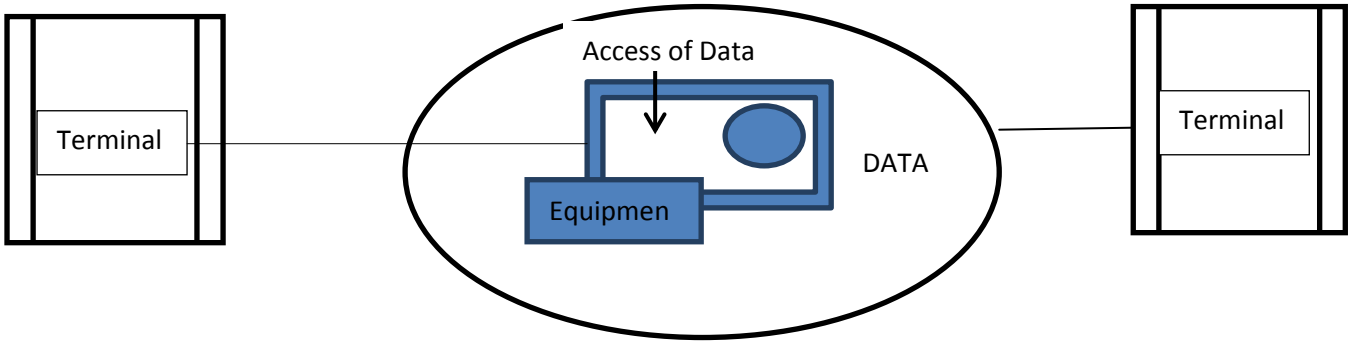

Fig 6:-Data

5. EXAMPLE OF MAPPING MODELS

5.1 VPN

Security issues associated to Virtual Private Networks can be analyzing as follows.

- Gateway control -An issue related to the security of multiple networks is controlling

  intentional or accidental access between logically private networks. This is related to the security functions of private networks ().

- Path control -An issue related to single networks is path assurance inside physical networks. This is related to the security functions each network possesses.

- Resource access control -An issue related to telecommunications equipment is security against access to one private networks resource by another private network.

- Data Access control -An issue related to data is security against improperly accessing various data that regulate VPNs. This is related to system security functions that control VPN data. At the same time, each private network should provide security against improper access to VPN Data.

5.2 CUG

Security issues related to CUG can be analyzed as follows.

- Gateway control -An issue related to security between multiple networks is controlling access to logical networks in which access between each CUG (including access between CUG's and general customers) is different. This is related to each CUG's security functions.

- Path control -An issue related to single networks is security related to the path settings between terminals.

- Resource access control -An issue related to telecommunications equipment is security against improperly accessing that equipment.

- Data access control -An issue related to data is security against improperly accessing various data that control and manage VPNs. This is related to system security functions that control VPN data. At the same time, each private network should provide security against improper access to VPN data.

5.3 Network Interference

Network interference has recently become a serious problem. High traffic access, intentional or accidental, paralyzes the functioning of telecommunications equipment or its networks. This problem can be analyzed as follows.

- Gateway control-An issue related to inter networks is controlling access from other networks that paralyze the functioning of one's own network. This is related to the security functions that each network possesses.

- Path control-An issue related to single networks is security related to access from terminals that paralyzes network functioning. This is related to securing paths.

- Resource access control- An issue related to telecommunications equipment is security related to access that paralyzes the functioning of that equipment. Each telecommunications device must be able to terminate access temporarily as soon as such disabling access is detected.

- Data access control-Finally, there is also an issue related to data. Improper accessing of data in telecommunications equipment may paralyze the functioning of that equipment and of the network.

5.4 Data Operation

An Intelligent Network service and network administration system has accumulated huge private, commercial and group data inside networks. By using these data, new services and control functions can be provided. Issues related to such data operations can be analyzed as follows

- Gateway control -An issue related to security between multiple networks is controlling improper access that executes improper operations on data in one's own network, which have been obtained from other networks.

- Path control- An issue related to single networks is the automatic detection and prevention of paths that cause improper data operations.

- Resource access control - An issue related to telecommunications equipment is security related to improperly accessing data stored in that equipment.

- Data access control -An issue related to data is improper data operation. This concerns preventing improper data operations or developing a fail-safe function against improper data operations.

6. CONCLUSION

This paper has proposed a network security approach, which goals to provide common conceptual network security in the Access model and a shared theoretical understanding for researchers. This proposed model divided into four levels and five sub-models, the model maps the distinct security issues and then treats them integrally.

7. REFERENCES

[1] Bell D.E. and LaPadulaL.J.,"Secure Computer System:Unified Exposition and Multics Interpretation", MiterMTR-2997(March 1976)

[2] SynderL.,"Formal Models of Capability-BasedProtectionSystems", IEEE Trans. on Computers, C30,3,pp.172-181(March 1981).

[3] Clark D.D. and Wilson D.R.,"A Comparison of Commercial and Military Computer Security Policies",IEEESymp.on Security and Privacy, pp.184-194 (1987).

[4] Brewer D.F.C. and Nash M.J.,"TheChineseWallSecurityPolicy", IEEE Symp. on security and Privacy, pp.206-214 (1989)

[5] Robert Koch, Björn Stelte, Mario Golling, “Attack Trends in Present Computer Networks”, 4th International Conference on Cyber ConflictC. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 .

[6] D. Denning, Information Warfare and Security,P163-183, Addison-Wesley Publishers, 1999.

[7] K. An Liu,R. Peng Ning, D. Maughan, Securing Network Access in Wireless Sensor Networks, WiSec'09, March 16 9,2009, Zurich, Switzerland. Copyright 2009 ACM 978-1- 60558-460-7/09/03

[8] Y. Y. Carsten Maple, "Reliability, Availability and Security of Wireless Networks in the Community," Informatica, p. 8, 2007.