Important Measures and Parameters for Establishing a Secure Network

SHOBAN BABU SRIRAMOJU[1] & DR. GYANENDRA KUMAR GUPTA[2]
[1]Research Scholar, Kalinga University, Raipur, India
[2]Associate Professor, Kalinga University, Raipur, India

Received: February 17, 2019 Accepted: March 30, 2019

ABSTRACT: *Supplying secure communication to maintain the consumer's data and apparatus secure when linked wirelessly has come to be one of the serious concerns. The security risks are rising day by day and creating top speed wired/wireless community and services, unreliable and insecure. Today -- a - times security measures functions more significantly towards satisfying the cutting edge demands of the growing businesses. The requirement can be triggered into the areas like protection, where protected and authenticated accessibility of tools are the vital issues associated with data security. Within this paper writer has clarified the vital steps and parameters concerning big industry/organizational prerequisites for developing a safe network. This paper investigates significant security measures associated with different network situations, to ensure a totally bonded network environment may be established within a business.*

Key Words: *Network Security, Wireless Network, Secure Network*

I. OVERVIEW OF WIRELESS NETWORKS

Wireless Networks

In the present age, everybody wants their essential data to be convenient, portable, accessible from virtually every area they see through the afternoon and this can be made possible by employing wireless networks. Wireless networks [1], as its name implies, are those programs which aren't linked with any physical means like Ethernet wires and so supply the consumer with fantastic freedom and convenience. In addition, it saves you from the costs on the wires which would be demanded if wired system is selected and makes it a lot easier for transferring the bottom of these apparatus from place to another by simply moving the device together with the wireless card.

A wired system aids in point to point move, which is, sends information between any two devices which are linked with each other via an Ethernet cable however in the event of wireless networks, even the transport of information is an air service in which the information is transmitted to all probable instructions in the moderate within a restricted variety because the medium of information transfer is atmosphere here rather than wires. Wireless networks include four primary elements: Transmission of information utilizing air wavesand access points (AP) to set a link to the private or public (business) system and the wireless customer run by the consumer. Fig. 1. Shows the Simple wireless network components.

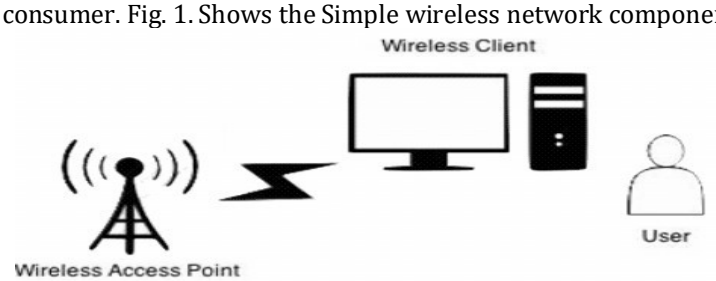

Figure 1. Wireless Networking Components

Security Issues in Wireless Networks

Wireless networks don't guarantee quality of support through transmission and opportunities of intrusion to these networks are extremely high because the transmission takes place via the medium of atmosphere rather than wires. Thus, it does not only demand protection against unauthorized users from accessing the system but also has to protect the consumers' personal data that's being sent.

1) **Confidentiality:** Your information being sent throughout the network is encrypted during transit in order to make sure that the info is read only by the user and consequently authentication of the recipient is necessary as well who'll receive the key to the decryption of the obtained information.
2) **Integrity:** Wireless systems are vulnerable to attacks which would damage the information's integrity.
   The ethics prevention methods implemented are like the ones used in wired systems.
3) **Entry:** Wireless systems are susceptible to denial of service attacks. Radio jamming may be utilized to limit the access to network. Another assault known as, battery exhaustion attack can be arisen where handicapped users send data or messages to associated devices and thus runs the device's battery life.
4) **Eavesdropping and Authentication:** Wireless systems are broadcasting as stated previously hence there are several access points and all these access points may be utilized to go into the network.
5) **Blue Snarfing or Blue Tooth:** All these are the attacks created with Bluetooth so as to tamper info or information theft.
6) **War Driver:** Another kind of security attack by which a wireless apparatus (such as laptops) somehow attempts to link to unprotected network and might capture the personal information of the consumer attached to the identical network.

Protocols in Wireless Networks

You will find wireless system protocols designed to be able to offer privacy security of the consumer information by encrypting the information being sent throughout the network. WLANs are described under the IEEE802.11 standard [3]. Table 1 outlines the three leading wireless security protocols.

Table 1. Wireless Security Protocols

Protocol	Full Form	Description
WEP	Wired Equivalent Privacy	Security similar to wired networks. Provides 10 to 26 long key. Easily broken security algorithm with numerous flaws.
WPA	Wi-Fi Protected Access	Uses Pre shared Key (PSK) and temporal key integrity protocol [4] for encryption of data.
WPA2	Wi-Fi Protected Access V.2	Uses Advanced Encryption Standards (AES) [5] for encrypting data.

The safety of a WLAN is contingent on the secrecy of the whole encrypting and decrypting procedure. Numerous algorithms are now employed for encrypting and decrypting without hastening the safety of the information being shipped. The design and evaluation of different mathematical techniques for encryption/decryption of Information that guarantee secure communications is known as as cryptography.

II. Attacks

Sensor networks are especially vulnerable to many important kinds of attacks. Attacks can be carried out in various ways, most especially due to denial of service attacks, but also through traffic investigation, privacy breach, physical attacks, and so forth.

On account of the possible asymmetry in computational and power limitations, protecting against a nicely orchestrated denial of service attack on a wireless sensor system could be just about impossible. A more potent node can quickly muster a sensor node and efficiently stop the sensor system from function - ing its planned responsibility.

We notice attacks on wireless sensor networks aren't confined to only type of service attacks, but instead encompass many different techniques such as node takeovers, attacks on the routing protocols, and also attacks to a node's physical safety. In this section, we address a few Frequent denial of service attacks then describe additional attacking, such as those about the routing protocols in Addition to an identity established attack Called the Sybil attack.

Types of Denial of Service attacks

A normal attack on wireless sensor networks would be just to shake a node or group of nodes. Jamming, in this circumstance, is the transmission of a radio signal which interferes with the radio frequencies used by the sensor system. The design of a system may come in two types: continuous jamming, and irregular jamming. Constant jamming requires the comprehensive jamming of the whole network. No messages can be received or sent. In case the jamming is just irregular, then nodes can exchange messages occasionally, but not always.

Attacks may also be produced on the connection layer itself. Such collisions will necessitate the retransmission of any warehouse influenced by the crash. With this tech- nique it might be feasible for the attacker to just deplete a sensor node's energy source by forcing a lot of retransmissions.

In the routing layer, a node can make the most of a multihop system simply by refusing to track messages. This might be carried out intermittently or continuously together with the net result being any neighbor that paths throughout the malicious node will be not able to exchange messages , at least, a part of their community.

The transport layer can be prone to attack, as in the instance of flooding. Flooding is often as straightforward as sending many link requests to a vulnerable node. In cases like this, resources have to be allocated to deal with the connection request. Finally a node's funds will be drained, thus producing the node futile.

The Sybil attack

Newsome et al. explain the Sybil attack because it pertains to wireless sensor networks. In other words, that the Sybil attack is described as a "malicious p-vice illegitimately carrying on several identities". It was initially described as a attack capable to conquer the redundancy mechanics of distributed information storage methods in peer reviewed systems. Along with beating distributed data storage methods, the Sybil attack can also be effective against routing calculations, information aggregation, voting, reasonable resource allocation and foiling misbehavior detection. Every one the techniques entail using numerous identities. For example, at a sensor system voting strategy, the Sybil attack could use numerous identities to create additional "votes". Likewise, to attack the routing protocol, the Sybil attack could rely upon a malicious node according to the identity of numerous nodes, and consequently routing Several paths via one malicious node.

Traffic Analysis Attacks

Wireless sensor networks are generally composed of numerous low-power sensors communicating using some comparatively robust and potent base stations. It's not uncommon, so, for information to be accumulated by the nodes in which it's finally routed into the bottom channel. Frequently, to get an adversary to efficiently render the system useless, the attacker can only disable the bottom channel. To make things worse, Deng et al. shows that could determine the base station in a community (with high probability) without actually comprehending the contents of these packets (when the packets are encrypted).

A speed monitoring attack only uses the thought that nodes nearest to the base channel are inclined to forward more packets than people further away from your base station. An attacker need only track that nodes are sending sticks and adhere to these nodes which are sending the many packets. To create an occasion, the adversary could only create a physical event which could be monitored from the sensor(s) at the region (turning to a light, for Example).

Node Replication Attacks

Conceptually, a node replication attack is rather easy: an attacker attempts to bring a node into an current sensor network by replicating (replicating) that the node ID of an current sensor node. A node replicated within this manner can seriously disrupt a sensor system's functionality: packets could be corrupt or perhaps misrouted. This could lead to a disconnected system, false sensor readings. When an attacker could obtain physical access to the full system he can replicate cryptographic keys into the duplicated sensor and may also insert the duplicated node into strategic issues in the community. By integrating the duplicated nodes in particular community issues the attacker could easily control a Particular Section of the network, possibly by disconnecting it entirely.

Attacks Against Privacy

Sensor network technologies guarantees a huge growth in automatic information collection capacities through efficient setup of miniature sensor devices. When these technologies provide great advantages to consumers, they also display significant possibility of misuse. Particularly related issues are privacy troubles, because sensor networks supply increased information collection capacities.

The principal privacy difficulty, nevertheless, isn't the sensor networks permit the selection of data. In reality, much info from sensor net- functions could most likely be accumulated through direct website surveillance. Instead, sensor networks exacerbate the privacy issue since they make large quantities of data readily available through remote access. Therefore, adversaries do not need to be physically present to keep surveillance. Remote access also enables one adversary to track a number of websites concurrently [11].

Monitor and Eavesdropping This really is definitely the most apparent attack to solitude. By listening to this information, the adversary may easily find the communication contents. After the traffic communicates the management information regarding the sensor system setup, which contains maybe more thorough information than reachable through the lo- cation machine, the eavesdropping can operate efficiently against the solitude security.

Traffic Analysis traffic analysis normally combines with observation and eavesdropping. A rise in the amount of switches between specific nodes could indicate a particular sensor has enrolled action. Throughout the study about the traffic, a few sensors with specific characters or actions can be efficiently identified. It's worth noting , as mentioned in the present Comprehension of solitude in wireless sensor networks is more immature, and much more study is required.

Physical Attacks

Sensor networks typically work in hostile outside surroundings. In these surroundings, the little form factor of these sensors, coupled together with the unattended and dispersed nature of the setup make them highly prone to physical attacks, i.e., dangers as a result of bodily node destructions. Unlike a number of different attacks mentioned previously, physical attacks ruin sensors forever, hence the losses are permanent. Recent work has revealed that regular sensor nodes, like the MICA2 motes, may be compromised in under 1 minute. When these results aren't surprising since the MICA2 lacks tamper resistant hardware security, they supply a cautionary note regarding the rate of an well-trained attacker. When an adversary interrupts a sensor node then the code in the physical node could be altered.

III. Network Security Measures

- A powerful firewall and firewall to be employed to help keep out unwanted people.
- A powerful Antivirus software bundle and Internet Security Software bundle ought to be set up.
- When employing a wireless link, utilize a password that is robust.
- Workers ought to be cautious regarding physical safety.
- Train a system analyzer or system screen and utilize it when required.
- Implementation of bodily security measures such as closed circuit tv for entrance places and limited zones.
- Security challenges to limit the company's perimeter.
- Fire asphyxiators may be used to get fire-sensitive regions including server rooms and safety rooms.

IV. Network Security Tools

- N-map Safety Scanner is a totally free and open source utility for network exploration or security auditing.
- Nessus is your finest free network vulnerability scanner on the market.
- Cable shark Ethereal is an open source network protocol analyzer for UNIX and Windows.
- Snort is light-weight system intrusion detection and avoidance system excels in traffic analysis and packet logging on IP networks.
- Web Cat is an easy utility which reads and writes data across TCP or UDP network links.
- Kismet is a strong wireless sniffer.

V. SECURITY MANAGEMENT ISSUES

- strengthening the safety strength of this business is a large challenge today. Organizations possess a few predefined safety policies and processes but they aren't implementing it so. Through the usage of technologies, we ought to impose those policies on process and people.
- Construction and affirming high-tech tools for installation and efficient control of network security infrastructure.
- Adopting technologies which are simple and cost effective to install and handle day-to--afternoon network security surgeries and troubleshoots at the very long term.
- Ensuring a totally protected network environment with no degradation in the operation of business programs.

- On an everyday basis, corporations face the challenge of needing to scale their infrastructure up into a rapidly growing user category, either from inside and beyond those associations. At exactly the exactsame time they also need to make sure that functionality isn't compromised.
- Organizations occasionally need to take care of several stage products in the community. Securing them completely while ensuring smooth functionality is just one of the largest challenges that they face while preparing and executing a safety regimen.
- The execution and conceptualization of safety routine is a struggle. Safety is a mixture of people, procedures, and engineering; whereas IT managers are tuned to tackle just the tech controllers.

Network Security cuts across all purposes and therefore initiative and comprehension in the very top level is indispensable. Safety can be critical in the grassroots level and also to make sure this, worker awareness is a large concern. Being upgrade about the numerous choices and the fragmented marketplace is a struggle for many IT managers. In the security area, the operational period assumes a larger significance. Compliance also plays an active part in safety; therefore the business development staff, fund, as well as the CEO's office must matrix together with IT to provide a blueprint.

VI. SECURITY METHODS

a. Cryptography

- The most commonly used instrument for procuring services and information [11].
- Cryptography is based on ciphers, that can be nothing but mathematical functions used for encryption and decryption of a message.

b. Firewalls

A firewall is only a set of elements that jointly form a barrier between two different networks. [8,11] There are 3 basic Kinds of firewalls:

1) Application Gateways

Here is the primary firewall and can be a few times also called proxy gateways as shown at figure 2. These comprise of bastion hosts in order that they do behave as a proxy host. This Program runs in the Application Layer of this ISO/OSI Reference Model. Clients on the other side of the firewall has to be categorized & Assessing to be able to avail the services. This is the most protected, because it doesn't permit anything to pass default, but it also Have to Have the software composed and turned on so as to start the traffic departure.

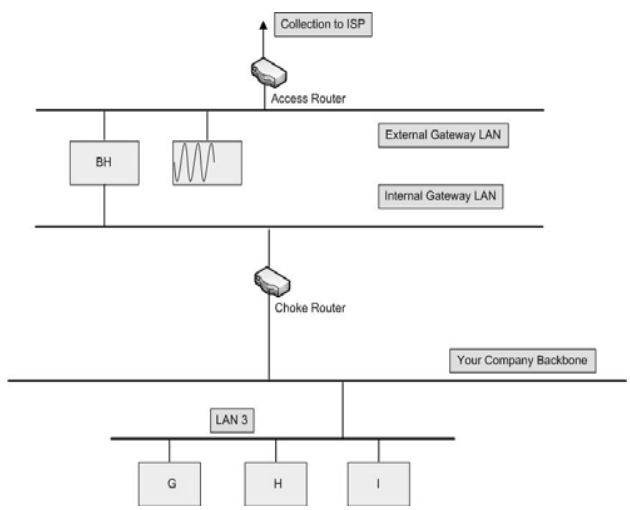

Figure 2: A sample application gateway

2) Packet Filtering

By default, a router will automatically pass all traffic routed through it, with no constraints as displayed in figure 3. ACL's is a system to specify exactly what kinds of access is permitted for the external world to need to get internal network, and vice versa.

This is significantly less complicated than an application entry, since the characteristic of access management is done in a decrease ISO/OSI layer. As a result of reduced sophistication and the reality that packet filtering is performed with routers, that can be technical computers optimized for jobs associated

with media, a packet filtering gateway is usually considerably quicker than its program coating cousins. Working in a lower degree, encouraging new programs either comes mechanically, or is a very simple matter of letting a particular packet type to maneuver through the gateway. There are issues with this technique; believed TCP/IP has no way of guaranteeing the origin address is what it claims to be. Consequently, utilize layers of packet filters are all have to in order to localize the visitors.

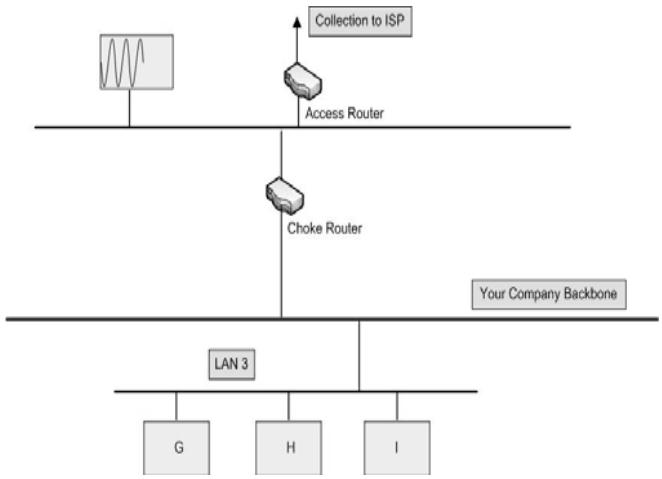

Figure 3: A sample packet filtering gateway

It could differentiate between a warehouse which originated from the net and one which originated from our internal system. Additionally It could be identified that network the packet originated from certainty, but it can not get more special than this.

3) Hybrid Systems

In an effort to unite the safety characteristic of the software layer gateways using all the speed and flexibility of packet filtering, a few programmers have established systems which use the fundamentals of the two. In a few of the systems, new relations have to be authenticated and accepted in the software layer. After this was completed, the rest of the link is passed to the session layer, in which packet filters see the link to make sure that only packets which are a part of a continuing (already endorsed and accepted) dialogue happen to be passed.

Programs of packet filtering and application layer proxies would be another potential ways. The advantages here comprise supplying a measure of security from the own machines which provide services to the Web (for instance, a public site), in addition to supply the safety of an application layer gateway into the internal system. Furthermore, using this technique an attacker, so as to access services on the inner system, Will Need to split the entry door, both the bastion host, along with the choke router.

VII. CONCLUSION

The main objective of the research work will be to demonstrate a system to enhance the safety element of WLANs. Safety is now significant issue for big computing businesses. There are various definitions and thoughts to the safety and risk measures from the view of unique individuals. Writer have proven the minimal set of prerequisites parameters to set a safe network environment for virtually any company with the support of the case analysis of an application development company. Security policies Shouldn't Be fixed as opposed to it must be adaptable enough to meet the requirement of a company and It Ought to Be able to handle potential safety threats while at Precisely the Same time readily manageable and adoptable.

REFERENCES

1. Brenton, C. and Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley
2. Farrow, R., Network Security Tools, found at http://sageweb.sage.org/pubs/whitepapers/farrow.pdf
3. Flauzac, O.; Nolot, F.; Rabat, C.; Steffenel, L.-A., “Grid of Security: A New Approach of the Network Security”, In Proc. of Int. Conf. on Network and System Security, 2009. NSS '09, pp. 67-72, 2009.
4. Stallings, W. (2006): Cryptography and Network Security, Fourth Edition, Prentice Hall.
5. Stallings, W. (2007): Network security essentials: applications and standards, Third Edition, Prentice Hall.

6. Wuzheng Tan; Maojiang Yang; Feng Ye; Wei Ren, A security framework for wireless network based on public key infrastructure, In Proc. of Computing, Communication, Control, and Management, 2009. CCCM 2009, Vol. 2, pp. 567 – 570, 2009
7. Sugandhi Maheshwaram, "A Review on Deep Convolutional Neural Network and its Applications" in "International Journal of Advanced Research in Computer and Communication Engineering", Vol. 8, Issue No. 2, February-2019 [ISSN : 2278-1021], DOI 10.17148/IJARCCE.2019.8230
8. N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location- support system. In Proc. of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MOBICOM), August 2000.
9. B. Przydatek, D. Song, and A. Perrig. Sia: Secure information aggregation in sensor networks, 2003.
10. S. Rafaeli and D. Hutchison. A survey of key management for secure group communication. ACM Comput. Surv., 35(3):309–329, 2003.
11. K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim. Highly reliable trust establishment scheme in ad hoc networks. Computer Networks: The Interna- tional Journal of Computer and Telecommunications Networking, 45:687–699, August 2004.
12. N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In ACM Workshop on Wireless Security, September 2003.
13. I.Sato, Y. Okazaki, and S. Goto. An improved intrusion detection method based on process profiling. IPSJ Journal, 43(11):3316–3326, 2002.
14. B. Schneier. Applied Cryptography. Second Edition, John Wiley & Sons, 1996.
15. A.Seshadri, A. Perrig, L. van Doorn, and P. Khosla. Swatt: Software-based attestation for embedded devices. In In Proceedings of the IEEE Symposium on Security and Privacy, May 2004.
16. Yeshwanth Rao Bhandayker, "AN OVERVIEW OF THEINTEGRATION OF ALL DATA MINING AT CLOUD-COMPUTING" in "Airo International Research Journal", Volume XVI, June 2018 [ISSN : 2320-3714]
17. Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198
18. Yeshwanth Rao Bhandayker , "Artificial Intelligence and Big Data for Computer Cyber Security Systems" in "Journal of Advances in Science and Technology", Vol. 12, Issue No. 24, November-2016 [ISSN : 2230-9659]
19. Sugandhi Maheshwaram, "A Comprehensive Review on the Implementation of Big Data Solutions" in "International Journal of Information Technology and Management", Vol. XI, Issue No. XVII, November-2016 [ISSN : 2249-4510]
20. Ajmera Rajesh, Siripuri Kiran, " Anomaly Detection Using Data Mining Techniques in Social Networking" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1268-1272 [ISSN : 2321-9653], www.ijraset.com
21. Sugandhi Maheshwaram , "An Overview of Open Research Issues in Big Data Analytics" in "Journal of Advances in Science and Technology", Vol. 14, Issue No. 2, September-2017 [ISSN : 2230-9659]
22. Siripuri Kiran, Ajmera Rajesh, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 637-642, [ISSN(ONLINE): 2395-1052]
23. Yeshwanth Rao Bhandayker, "Security Mechanisms for Providing Security to the Network" in "International Journal of Information Technology and Management", Vol. 12, Issue No. 1, February-2017, [ISSN : 2249-4510]
24. Sugandhi Maheshwaram, S. Shoban Babu , "An Overview towards the Techniques of Data Mining" in "RESEARCH REVIEW International Journal of Multidisciplinary", Volume-04, Issue-02, February-2019[ISSN : 2455-3085]
25. Yeshwanth Rao Bhandayker , "A Study on the Research Challenges and Trends of Cloud Computing" in "RESEARCH REVIEW International Journal of Multidisciplinary ", Volume-04, Issue-02, February-2019 [ISSN : 2455-3085]
26. Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications", Volume 1, Issue 1, Jan-Mar 2014 [ISSN : 2349-0020]
27. Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].
28. Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management", Volume VI, Issue I, Feb 2014 [ISSN : 2249-4510]