© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 02 | 25 | April - June 2016

THE REVIEW PAPER ON ENHANCEMENT OF WIRELESS SECRUITY

[1]Sonu. department of CSE, Om Institute of Technology & Management, Juglan, Hisar
[2]Neeraj Verma, department of CSE, Om Institute of Technology & Management, Juglan, Hisar

Abstract: most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over network. Most wireless routers, access points, & base stations have a b uilt-in encryption mechanism. If our wireless router doesn't have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with encryption feature turned off. So we need to educate individuals & organizations on how to optimal use safety features. In this research we have enhanced wireless network by introducing triple layer security mechanism.

Keywords: RF, PCS, LAN,MAN,WAN

[I] Introduction.

Wireless local area network technology are widely deployed & used in organisations today. Using radio frequency (RF) technology, wireless LANs transmit & receive data over air, minimising need for wired connections. Thus, wireless LANs combine data connectivity with user mobility. Wireless networking is a method by which homes, telecommunications networks & enterprise installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented & administered using radio communication. This implementation takes place at physical level of OSI model network structure.

Examples of wireless networks include cell phone networks, Wi-Fi local networks & terrestrial microwave networks.

[2] Various wireless network systems

1. *Terrestrial microwave* :– Terrestrial microwave communication uses Earth-based transmitters & receivers resembling satellite dishes. Terrestrial microwaves are in low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km apart.
2. *Cellular & PCS systems* use several radio communications technologies. systems divide region covered into multiple geographic areas. Each area has a l ow-power transmitter or radio relay antenna device to relay calls from one area to next area.
3. *Radio & spread spectrum technologies* :– Wireless local area networks use a high-frequency radio technology similar to digital cellular & a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology known as Wifi.
4. *Free-space optical communication* uses visible or invisible light for communications. Line-of-sight propagation is used, which limits physical positioning of communicating devices.
5. *Communications satellites* :– Satellites communicate via microwave radio waves, which are not deflected by Earth's atmosphere. satellites are stationed in space, typically in geosynchronous orbit 35,400 km above equator.se Earth-orbiting systems are capable of receiving & relaying voice, data, & TV signals.
6. *Terrestrial microwave* :– Terrestrial microwave communication uses Earth-based transmitters & receivers resembling satellite dishes. Terrestrial microwaves are in low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km apart.

7. *Cellular & PCS systems* use several radio communications technologies. systems divide region covered into multiple geographic areas. Each area has a l ow-power transmitter or radio relay antenna device to relay calls from one area to next area.
8. *Radio & spread spectrum technologies* :– Wireless local area networks use a high-frequency radio technology similar to digital cellular & a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology known as Wifi

[3] Threats to Wireless Network

Security exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in website/domain hacking.
Hacking Techniques

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Firewalls defend computers from intruders by limiting access to ports and machines, but they can still be circumvented.)

Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (Phishing)

A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying data and is thereby treated as a t rusted system by a user or another program—usually to fool programs, systems or users into revealing confidential information, such as user names and passwords.

[4] Research Methodology

Packet filtering is a firewall technique used to control network access by monitoring outgoing & incoming packets & allowingm to pass or halt based on source & destination Internet Protocol (IP) addresses, protocols & ports.

Network layer firewalls define packet filtering rule sets, which provide highly efficient security mechanisms.

Packet filtering is also known as static filtering. User Datagram Protocol (UDP) is part of Internet Protocol suite used by programs running on different computers on a network. UDP is used to send short messages called datagrams but overall, it is an unreliable, connectionless protocol. User datagram protocol is an open systems interconnection (OSI) transport layer protocol for client- server network applications. UDP uses a simple transmission model but does not employ handshaking dialogs for reliability, ordering & data integrity. protocol assumes that error-checking & correction is not required, thus avoiding processing at network interface level.

UDP is widely used in video conferencing & real-time computer games. protocol permits individual packets to be dropped & UDP packets to be received in a d ifferent order than that in whichy were sent, allowing for better performance. U DP network traffic is organized in form of datagrams, which comprise one message units. first eight bytes of a datagram contain header information, while remaining bytes contain message data. A UDP datagram header contains four fields of two bytes each:

1. Source port number
2. Destination port number
3. Datagram size

4. Checksum
5. Development of firewall code is based on following steps
6. Extract packet header
7. Check protocol associated
8. Compare with rules
9. Check source & destination add. If protocol is same
10. Check out port if protocol is TCP
11. Drop or pass packet

[5] Objectives

Our objective is to follow integrated approaches Cryptography & Firewall. Firewall will filter un athenticated data & Cryptography will make information difficult to understad for Intruder or Hacker in wire less Network Threats. The objective is to provide triple layer security.

- Enhancement of existing encryption algorithm.
- Applying IP filter to enhance security. Protection against various threat is motto of research.
- Establishment of application based security to user by proving login/password & OTP based mechanisms.
- Most threats against wireless networks involve an attacker with access to radio link between wireless devices. Several of threats listed below rely on an attacker's ability to intercept & inject network communications.

For a wired network, an attacker would have to gain physical access to network or remotely compromise systems on network: for a wireless network, an attacker simply needs to be within range of wireless transmissions.
Another common threat against wireless networks is deployment of rogue wireless devices. For example, an attacker could deploy a device, most likely a r ogue AP that has been configured to appear as part of an organisation's wireless network infrastructure.

[6] PROPOSED MODEL

In proposed model there would be triple layered security

- Security layer 1 would be customized cryptography algorithm of AES to enhance security.
- Security layer 2 would drop packets from authentic IP addresses.
- Security layer 3 would authenticate user by providing login password security at application layer.
- Security would be enhanced using one time password also that becomes useless after using one time.

In this way we will secure wireless network from external attacks and authentic access.

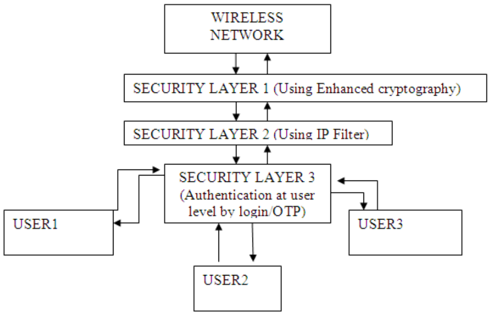
WIRELESS NETWORK
SECURITY LAYER 1 (Using Enhanced cryptography)
SECURITY LAYER 2 (Using IP Filter)
SECURITY LAYER 3 (Authentication at user level by login/OTP)
USER1
USER2
USER3

Fig 1. Proposed model

[7] SCOPE AND CONCLUSION

Security is a very complex topic. We are following integrated approaches Cryptography and Firewall. Firewll will filter un athenticated data and Cryptography will make information difficult to understad for Intruder or Hacker in wire less Network. It is very important to build systems and networks in such a way that the user is not constsntly remainded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. From all the available distributed and centralized systems, four most commonly used distributed systems were discussed in depth and then the security issues faced by these systems and the solutions proposed by various researchers were discussed in depth. Finally the security issues and solutions proposed for different systems were summarized and compared with each other.

REFERENCES

1. Sangita A. Jaju, Santosh S. Chowhan," **A Modified RSA Algorithm to Enhance Security**

for Digital Signature", 978-1-4799-6908-1/15©**2015 IEEE**.

2. Ayman Tajeddine Ayman Kayssi Ali Chehab Imad Elhajj," **Authentication Schemes for Wireless Sensor Networks**", 17th IEEE Mediterranean Electrotechnical Conference, Beirut, Lebanon, 13-16 April 2014. 978-1-4799-2337-3/14©**2014 IEEE**.
3. Natasha Saini1 ,Nitin Pandey2, Ajeet Pal Singh3," **Enhancement Of Security Using Cryptographic Techniques",** 978-1-4673-7231-2/15©**2015 IEEE**.

4. Ashwak alabaichi, Adnan Ibrahem Salih, "**Enhance Security of Advance Encryption Standard Algorithm Based on Key-dependent SBox**", ISBN: 978-1-4673-6832-2©**2015 IEEE**.

5. Kyung-Ah Shim," **A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks**" IEEE Communications Survey & Tutorials, Vol., No., 2012, 1553-877X (c) **2015 IEEE**.

6. Madhumita Panda, Atul Nag, "**Plain Text Encryption Using AES, DES & SALSA20 by Java Based Bouncy Castle API on Windows & Linux",** 2015 Second International Conference on Advances in Computing & Communication Engineering, 978-1-4799-1734-1/15 © 2015 IEEE DOI 10.1109/ICACCE.2015.130.

7. Jian Shen, Haowen Tan, Sangman Moh, Ilyong Chung, Qi Liu, & Xingming Sun," **Enhanced Secure Sensor Association & Key Management in Wireless Body Area Networks**", Journal Of Communications & Networks, Vol. 17, No. 5, October 2015, 1229-2370/15c **2015 KICS**.

8. Michael Ekonde Sone," **Efficient Key Management Scheme to Enhance Security-Throughput Trade-off Performance in Wireless Networks**", Science & Information Conference **2015 July 28-30**.

9. B. Karthikeyan, M. V elumani, R. Kumar4 & Srinivasa Rao Inabathini3," Analysis of Data Aggregation in Wireless Sensor Network", **IEEE** Sponsored 2nd International Conference On Electronics & Communication System**(ICECS 2015)**.

10. Takahiro Fujita, Kiminao Kogiso, Kenji Sawada, & Seiichi Shin, "**Security Enhancements of Networked Control Systems Using RSA Public-Key Cryptosystem**", 978-1-4799-7862-5/15©**2015 IEEE**.

11. Prachi, Surbhi Dewan, Pratibha, **Comparative Study of Security Protocols to Enhance Security over Internet",** 2015 Fifth International Conference on Advanced Computing & Communication Technologies, 2327-0659/15© **2015 IEEE**.

12. Madhumita Panda**, "Data Security in Wireless Sensor Networks via AES Algorithm",** IEEE Sponsored 9th International Conference on Intelligent Systems & Control (ISCO)2015, 978-1-4799-6480-2/15©**2015 IEEE**.

13. Raghav Mathur, Shruti Agarwal," **Solving Security Issues in Mobile Computing using Cryptography Techniques -A Survey**", International Conference on Computing, Communication & Automation (ICCCA2015), ISBN:978-1-4799-8890-7/15©**2015 IEEE**.

14. Pravin Raj .S, A.Pravin Renold," **An Enhanced Elliptic Curve Algorithm for Secured Data Transmission In Wireless Sensor Network**", Proceedings of 2015 G lobal Conference on Communication Technologies(GCCT 2015), 978-1-4799-8553-1/15© **2015 IEEE**.

15. Antonio F. Skarmeta, Jos´e L. Hern´andez-Ramos, M. Victoria Moreno, "**A decentralized approach for Security & Privacy challenges in Internet of Things**", 2014 IEEE World Forum on Internet of Things (WF-IoT). 978-1-4799-3459-1/14©**2014 IEEE**.

16. Abdelbasset Trad, Abdullah Ali Bahattab, Soufiene Ben Othman," **Performance Trade-offs of Encryption Algorithms For Wireless Sensor Networks",** 978-1-4799-3351-8/14©**2014 IEEE.**

17. Hassan Noura, Steven Martin, Khaldoun Al Agha," **EDCA: Efficient Diffusion Cipher & Authentication Scheme for Wireless Sensor Networks**", IEEE WCNC'14 Track 3 (Mobile & Wireless Networks), 978-1-4799-3083-8/14©**2014IEEE**.

18. Abhilasha Naidu, A.Y.Deshmukh, Vipin Bhure, "**Design of High Throughput & Area Efficient**

Advanced Encryption System Core", International Conference on Communication & Signal Processing, April 3-5, 2014, India, 978-1-4799-3358-7114©**2014 IEEE**.

19. Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk," **A New Security Protocol Using Hybrid Cryptography Algorithms**", 978-1-4799-3370-9/13©**2013 IEEE**.

20. Hassan Noura, Steven Martin, Khaldoun Al Agha & Walter Grote"**Key Dependent Cipher Scheme for Sensor Networks**", 2013 12t h Ann,ual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET),, 978-1-4799-1004-5/13©**2013 IEEE**.

21. Miroslav Botta, Milan Simek, & Nathalie Mitton," **Comparison of Hardware & Software Based Encryption for Secure Communication in Wireless Sensor Networks**", 978-1-4799-0404-4/13©**2013 IEEE**.

22. Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef," **Performance Evaluation Of EncryptionAlgorithm For Wireless Sensor Networks",** 2012 International Conference on Information Technology & e-Services, 978-1-4673-1166-3/12©**2012 IEEE**.

23. Bhushan Chaudhari, Prathmesh Gothankar, Abhishek Iyer, D. D. Ambawade,"**Wireless Network Security Using Dynamic Rule Generation of Firewall**", 2012 I nternational Conference on Communication, Information & Computing Technology (ICCICT), **Oct. 19-20,2012**.