Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.808 – 813

The Review Paper on Securing Wireless Network from External Threats

Sonu[1], Surender Singh[2]

[1]Computer Science & Engg. Department, Om Institute of Technology & Management, Haryana, India

[2]Computer Science & Engg. Department, Om Institute of Technology & Management, Haryana, India

[1] soniajhajhria11@gmail.com, [2] surender.punia@yahoo.com

Abstract: 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. 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. Thus we have 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, SSL, FTP, TELNET"

[1] 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 low-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 low-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] Different Types Of Attack On Wireless Network

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur.

There are five types of attack:

Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Distributed Attack

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

Insider Attack

An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

Close-in Attack

A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

[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.

[5] Main Objectives of research

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

1. Enhancement of existing encryption algorithm.
2. Applying IP filter to enhance security. Protection against various threat is motto of research.
3. Establishment of application based security to user by proving login/password & OTP based mechanisms.
4. 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 rogue AP that has been configured to appear as part of an organisation's wireless network infrastructure.

[6] PROPOSED WORK

Security layers working as follow :-

- **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.

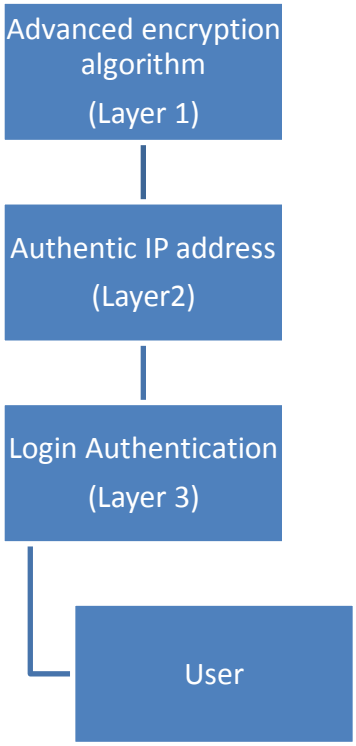

Fig 1 Multilayer Security

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

[7] SCOPE AND CONCLUSION

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. 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.

References:

1. Michael Ekonde Sone," Efficient Key Management Scheme to Enhance Security-Throughput Trade-off Performance in Wireless Networks", Science & Information Conference 2015 July 28-30.
2. Natasha Saini1 ,Nitin Pandey2, Ajeet Pal Singh3," Enhancement Of Security Using Cryptographic Techniques", 978-1-4673-7231-2/15©2015 IEEE.
3. 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.
4. Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk," A New Security Protocol Using Hybrid Cryptography Algorithms", 978-1-4799-3370-9/13©2013 IEEE.
5. Bhushan Chaudhari, Prathmesh Gothankar, Abhishek Iyer, D. D. Ambawade,"Wireless Network Security Using Dynamic Rule Generation of Firewall", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20,2012.
6. Sangita A. Jaju, Santosh S. Chowhan," A Modified RSA Algorithm to Enhance Security for Digital Signature", 978-1-4799-6908-1/15©2015 IEEE.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. B. Karthikeyan, M. Velumani, R. Kumar4 & Srinivasa Rao Inabathini3," Analysis of Data Aggregation in Wireless Sensor Network", IEEE Sponsored 2nd International Conference On Electronics & Communication System(ICECS 2015).
13. 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.
14. 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.
15. 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.
16. 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.
17. Pravin Raj .S, A.Pravin Renold," An Enhanced Elliptic Curve Algorithm for Secured Data Transmission In Wireless Sensor Network", Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015), 978-1-4799-8553-1/15© 2015 IEEE.

18. 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.
19. 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.
20. 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.
21. 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.
22. Hassan Noura, Steven Martin, Khaldoun Al Agha & Walter Grote"Key Dependent Cipher Scheme for Sensor Networks", 2013 12th Ann,ual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET),, 978-1-4799-1004-5/13©2013 IEEE.
23. 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.
24. 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.

