ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (48-51), Month: October - December 2015, Available at: www.researchpublish.com

Protection for Wireless Networks from Hazards and Vulnerabilities

KARTHEEK RAVULA[1], PARIMALA SOWMYA BODAPATI[2]

[1]Student of M. Tech (CSE) and Department of Computer Science Engineering,
[2] Student of M. Tech (CSE) and Department of Computer Science Engineering, Chirala Engineering College

Abstract: **Wireless Network accommodates several benefits, however it also clasp with recent security threats as well as change the organizations complete data security risk analysis. Even though utilization of methodological solutions is the common feedback to wireless security threats and vulnerabilities, wireless security is generally an administrative affair. Impressive management of the threats link with wireless technology need a sound and absolute evaluation of risk given the surroundings and growth of a scheme to check identified threats. We present a framework to assist managers understand and evaluate the miscellaneous threats associated with the use of wireless technology. In addition to confabulate a number of possible solutions for bilk those hazards.**

Keywords: **Wireless Network, Wireless Security, Threats, Wireless Technology.**

I. INTRODUCTION

Wireless Network accommodates several benefits, Work rate become well, because of raised approachability to information resources. Arrangement of network and re-arrangement is not difficult, speedy, and slighter high-priced. Anyhow, wireless technologies also compose fresh threats and change the actual information security risk profile, because exchanging information takes place “over the air” using electronic airwaves i.e., radio frequencies. Blocking risk is larger than with wired network. Message is not encrypted or encrypted with a decrepit algorithm, the attacker look at and understands the written word, thereby conciliate confidentiality. Even though changes the wireless networking risks correlate with miscellaneous hazards to security, the complete security aim leftover the same as with wired networks: secure the confidentiality, protect integrity, and maintain accessibility of the information systems. The aim of this paper is to help managers in shaping such decisions by supporting them with an elementary understanding of the character of the miscellaneous threats link with wireless networking and open to anti portion (Countermeasures).

The reputation of wireless networks is a testament basically to their availability, expensive capability, and mixing with other networks and network elements are so easy. The larger part of computers sold to buyers today with all essential wireless networks technology. Advantages of wireless network involve: Usefulness (Convenience), Mobility (Ability to move), Work rate (Productivity), Arrangement (Deployment), and Price. While complete with the availability and benefits described atop has its share of downfalls. For a given networking place of activity, networking like wireless may not be attractive for more number of reasons. The disadvantage of these technologies: safety-Protection (Security), Extent (Range), Dependability (Reliability), and Fast (Speed).

Today Wireless networks introduce moderate issues for network controllers. Unofficial entry points, SSIDs relay (broadcasting), obscure stations, and MAC address also spoof and having some few problems addressed in WLAN damage control (troubleshooting).

II. WIRELESS HAZARDS, VULNERABILITIES, AND OPPOSING MEASURES

It consists of four elementary components: Transmission of data was done by using radio frequencies; approaching points that support a connection to the administrative networks. Example: Laptops etc... Every element provides a route for hazard that means attack that can effect in the compromise of 3 essential basic security goals of secret, availability and integrity.

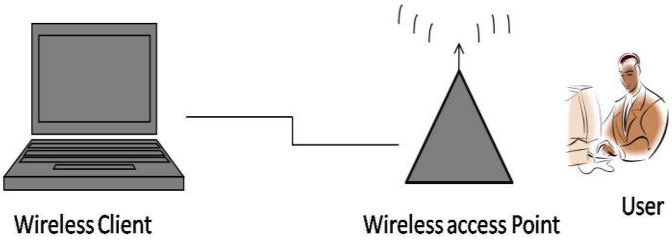

Fig.1. Components for wireless network

III. ATTACKS

In wireless networks mainly having nine components:

1. Accidental association
2. Malicious association
3. Ad-hoc networks
4. Non-traditional networks
5. Identity theft (MAC spoofing)
6. Man-in-the-middle attacks
7. Denial of service
8. Network injection
9. Caffe Latte attack

IV. PROTECTING WIRELESS TRANSMISSIONS

The wireless communications characterizes 3 fundamental threats: Blocking (Interception), repeated rotation (Alternation), interruption (Disruption).

Securing the Secrets Of Wireless Transmissions:

Having 2 types of opposing measures be exist for lowering the risk of monitor on transmission wireless. To draw the first method for making it more hard to come across and interrupt the signals of wireless. To draw the second method it involves the use of encryption to care for confidentiality.

Signal - concealing methods:

In order to head off Wireless transmissions, attackers 1st want to recognize and find network of wireless. Still, a number of steps that arrange to make it more painful to locate their wireless access point. The easiest, smooth and less costly contain the following: Switch off or turning off the service set identifier (SSID) telecast by wireless access points, select secret names to SSIDs, decreasing the signal stamina to the shortest level that still provides need coverage. More effectively, but in addition to more costly methods for decreasing or concealing signals.

Encryption:

The most excellent method for take care of the confidentiality of data, communicate over wireless networks is to encrypt whole quantity of wireless traffic. This is particularly essential for organizations subject to managing.

Impede alternation of intercepted communication:

Blocking (Interception) and changing (Alternation) the wireless transmission presents a shape of “Man in the middle” attack. Opposing measures are 2 types that can meaningfully make less the risk of such hazards. Powerful encryption and healthy authentication of twain devices and users.

Opposing Measures to Decrease the Risk of Denial of Service Hazards:

Wireless communications are open to attack in the direction of DOS attacks. Administrative can profit various steps to decrease the risk of specific not planned Denial of Service attacks. Careful site examines can recognize the specific region where indications (signals) from other devices exist; the result of specific scrutiny should be used when determining where to find wireless access locations. Proper cyclic audits of wireless networking movement and performance can recognize difficult scope of a surface; suitable restorative actions may contain elimination of the delinquent devices or measure to maximize the signal stamina and coverage with in the difficulty area.

Protecting Wireless Access Points:

Uncertain, not well set up wireless access points can compromise privacy by allowing unofficial approach to the network.

Opposing Measures To Balance Wireless Access Points:

Organizations can decrease the risk of unofficial access to the network of wireless having these 3 activities:

1. Removing fraud access points
2. Correctly set up all official access points and
3. Utilizing 802.1x to authenticate each and every device

Protecting wireless consumer or client device:

In wireless client devices mainly we have 2 bigger foremost threats are (1) Stealing or loss and (2) Compromise. Stealing or loss of computers, Laptops and PDAs is a serious bad situation. PDAs and laptops frequently store secret and control information. As a consequence, misfortune or stealing or loss of devices may cause organization to be breach of secrecy organizing draw in the announcement of personal identifying information it has collected from third parties.

Protecting wireless networks:

Encryption advantages:

The best persuasive method to protect your wireless network from intruder is to encrypt, or confusion or mix-up, system information exchange over the network. Maximum wireless routers and base stations have a in-built encryption techniques. Encryption characteristic’s doesn’t have in your wireless router look at one that does. Producers frequently distribute wireless routers with the encryption characteristics switched off or turned off. Definitely you turn it on.

Use Anti- Virus and Anti- Spyware software’s:

First a fall, every computer wants security for protecting the data. Protection is very important in all the networks not only wireless. Computer on the wireless network want protection on internet. Install anti-virus and anti-spyware software’s and update it regularly that means time-to-time. Turn on your firewall option in your computer when it is turned off.

List some of the Anti-virus Software’s:

1. Kaspersky
2. Norton
3. Web root
4. 360 security
5. Avast
6. AVG
7. ESET
8. MCA fee
9. Bit Defender
10. Avira etc…

List some of the Anti-Spyware Software’s:

1. Spybot Search and Destroy
2. Ad-Aware
3. Malwarebytes’ Anti-Malware
4. Spyware Blaster
5. Anti-Malware Suites etc...

V. TURN OFF BROADCASTING IDENTIFIER

Best wireless routers have a technique called recognition broadcasting. It transmits out a signal to each device in the local area make a proclamation its presence. Cyberpunk can use identifier broadcasting to domestic in on dangers wireless networks. Disable the recognition broadcasting techniques if your wireless router grant or allow it.

VI. CONCLUSION

Wireless networking supports abundant opportunities to raise the productivity and incision prices. In addition to alters an organization’s complete computer security risk outline. Even though it is beyond the bounds of possibility to completely delete each and every risk connected with wireless networking, it is possible to bring a reasonable level of complete security by adopting an orderly approach to evaluate and managing hazard or risk. This paper talks over about the threats, vulnerabilities connecting with each of 3 fundamental mechanism elements of wireless networks and explaining miscellaneous commonly ready for use of opposing measures that could be used to check those hazards. It also accentuates the importance of preparation and educating consumers in safe wireless networking procedures.

REFERENCES

[1] Graham, E., Steinbart, P.J. (2006) Wireless Security

[2] Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.

[3] CSI. (2004). CSI/FBI Computer Crime and Security Survey.

[4] Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.

[5] Kelley, D. (2003). The X factor: 802.1 xs may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.

[6] Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).

[7] McDougall, P. (2004, March 25). Laptop theft puts GMAC customers’data at risk. Information Week Security Pipeline.

[8] Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.

[9] Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols for wireless communications.

[10] Slashdot. (2002, August 18). Wardriving from 1500ft Up.

[11] Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk management guide for information technology systems. NIST Special Publication 800-30.

[12] Wailgum, T. (2004, September 15). Living in wireless denial. CIO Magazine.

[13] International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008

AUTHOR PROFILE

Kartheek Ravula, Presently pursuing his M.Tech in Computer Science & Engineering from Chirala Engineering College, Chirala, Prakasam District, A.P, India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, New Delhi. His B.Tech completed at VRS & YRN College of Engineering & Technology, Chirala, Prakasam District, A.P, India.

Parimala Sowmya Bodapati, Presently pursuing her M.Tech in Computer Science & Engineering from Chirala Engineering College, Chirala, Prakasam District, A.P, India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, New Delhi. Her B.Tech completed at Narasaraopeta Engineering College , Narasaraopet, Guntur District, A.P, India.