International Journal of Advanced Research in Engineering Technology & Science

ISSN: 2394-2819

Email: editor@ijarets.org Volume-3, Issue-5 May- 2016 www.ijarets.org

REVIEW PAPER ON MOBILE NETWORK AND THEIR SECURITY ISSUES

Ashu
Research Scholar
Dept. of Computer science
NIILM University Kaithal

Dr. Anil Kumar
Associate Professor
Dept. of Computer science
NIILM University Kaithal

ABSTRACT: The following paper is a literature review on the topic of mobile network and their security aspects. The topic has been chosen due to the rise in mobile applications and the insufficient rise in the security within those applications. For the purpose of this paper mobile networks are considered as wireless network which does not have any infrastructure. Security is a big issue in wireless network. Mobile networks are characterized by two attributes which impact end user perception about the quality of the service received. The malicious users use different techniques like Password cracking, sniffing unencrypted or clear text traffic etc. to exploit the system vulnerabilities .vulnerability is a weak spot which allow an attacker to decrease system's security. The firewall and the Intrusion detection system is a technique which protects system from malicious attacks. Wide spectrum of IDS is available, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network.

KEYWORDS- mobile network, security issues**,** intrusion detection, firewalls, vulnerability

INTRODUCTION

A mobile network is a communication network which is distributed over land areas called cells. Each cell is served by at least one fixed location transceiver known as cell site or base station. Cell sites and mobile devices manipulate the frequency so that they can make use of low power transmitters to supply their services with the leas possible interferences. In order for mobile networks to function they need a substantial network of base stations to provide sufficient radio coverage in any geographical area to handle customer voice, text or data. A mobile device converts data in to radio waves. These signals are transmitted from the device to the nearest base station. The radio waves that allow mobile devices to work are part of the electromagnetic spectrum, travelling from point to point at high speed.

LITERATURE REVIEW

Well-documented recent studies show that cyber-attacks continue to remain a substantial threat to organizations of all types. On average companies experience several dozen attacks per week on their IT resources. CarnCarnegie Lon University's computer emergency response team identified just fewer than 200 vulnerabilities in 2005 and 8064 in 2006. It has been conservatively forecasted that in 2010 around 10,000 new vulnerabilities will be discovered in software applications in that year alone. According to internet security threat report, in 2015, the number of zero-day vulnerabilities discovered more than doubled to 54, a 125 percent increase from the year before. Or put another way, a new zero-day vulnerability was found every week (on average) in 2015. Given the value of these vulnerabilities, it's not surprising that a market has evolved to meet demand. This will force companies to assess and mitigate one new risk every hour each day of the year.

Hyung-woo lee et al. explained various issues and challenges in wireless network. He explained two types of security attacks. One is the attack against the security mechanisms and another is against the basic mechanism like routing mechanism.

Lifeng Sang, et al. (2010) proposed shared secret free security infrastructure for wireless networks based on two physical primitives: cooperative jamming and spatial signal enforcement. Cooperative jamming is for confidential wireless communication and spatial signal enforcement is for message authenticity. Proposed infrastructure provides confidentiality, identity authentication, message authentication,

Floyd (2006) report that security is not important only in wired network but it is an important factor in any network including wireless network. He devised a cryptographic solution to secure mobile ad-hoc networks that are especially vulnerable to malicious attacks since they possess no clear line of defense.

NEED OF THE STUDY

Security is a challenging and important issue for wireless ad hoc networks. In wired networks however the attacker needs to gain access to the physical media e.g. network wiring etc. or pass through a plethora of firewalls and gateways. In wireless networks the scenario is quite different, there are no firewalls and gateways in place hence attacks can take place from all directions. Every node in the ad-hoc network must be prepared for dealing with the adversarial access attempts. Each mobile node in ad-hoc network is an autonomous unit, free to move independently. This means a node with inadequate physical protection is very much susceptible to being captured, hijacked or compromised. It is difficult to track down a single compromised node in a large network. Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. If users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk.

A mobile network needs to provide its nodes access to an internet and logically it does so by means of its mobile routers which are responsible for maintaining the mobile network's connectivity to the IP infrastructure. When a mobile network is on the move, its mobile router will need to change its point of attachment to the IP infrastructure while moving into and out of different network segments of the same or different access networks.

PROPOSED WORK

As the study explains that wireless network has no infrastructure so the security of wireless networks are big challenge for everyone. The IPv6 environment is most likely to be more important than the IPv4 environment for the support of mobile networks. IPv6 will change many things in different areas, because it is faster, more efficient and more scalable than IPv4 with the large address space, the auto configuration possibilities, and the extensibility provided by the extension header architecture.

OBJECTIVES OF THE STUDY

- To understand the network model and attacker model to design better security solutions.
- To understand intrusion prevention techniques like encryption and authentication for security purpose.
- To examine the various mobile networks to ensure the security.

RESEARCH METHODOLOGY

Research methodology used for this purpose is Key management; Ad-hoc routing and intrusion detection aspects of wireless Ad-hoc networks are used. The key management protocols are still very expensive. Several protocols for routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. Intrusion detection is a critical security area which is also concerned in the research. But it is a difficult goal to achieve in the resource deficient Ad-hoc environment. But the flexibility, ease and speed with which these networks can be set up implies they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. Intrusion detection on these complex systems is an evolving, immature research area. There are far fewer proposed IDSs for MANETs than for conventional networks. Researchers can focus on either introducing new IDSs to handle MANET specific features or can adapt existing systems. Suitability of the architecture to the environment is an important consideration in designing IDS. An architecture should not introduce new weaknesses/overheads to IDS. For instance, some of the proposed architectures like cluster-based approaches are costly to build and maintain for high-mobility networks and may also have critical points of failure. More intense detection algorithms are applied in order to monitor critical nodes. Testing IDS is also an open research area for both MANETs and conventional networks. Some of the proposed systems are tested only on very small networks and with few attack scenarios. IDSs are tested under different mobility levels and with different network topologies.

CONCLUSION

Different wireless networks are used in a country. But lack of any infrastructure they are not secure. Security is a major issue in wireless network as there are various threats which affect our system. Mobile security requires a different approach which leaves an area clear of opportunity for future scholarly research.

REFERENCES

1. Bradley, T. *Glossary*. http://netsecurity.about.com/library/ glossary/bldef-appg.htm.
2. BroadbandReports.com, dslreports.com. Does IPv6 introduce new security vulnerabilities? New York: Silver Matrix LLC, Feb, 15, 2008. http://www.broadbandreports.coml faq/ipvsixl 4.0 _IPv6 _Security.
3. CSO Online.http://www.csoonline.com/glossary/category.cfm?ID= 13.
4. Desmeules, R. *Cisco self-study: Implementing Cisco IPv6 Networks (IPv6).*Cisco Press, June 6, 2003.
5. Hermann-Seton, P. *Security features in IPv6*. SANS Institute 2002, as part of the Information Security Reading Room, 2002.
6. ICANN Security and Stability Advisory Committee (SSAC). *Survey of IPv6 support in commercial firewalls.* Oct. 2007.
7. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-today-tomorrow-341