Globus An International Journal of Management & IT
A Refereed Research Journal

Vol 11 / No 1 / Jul-Dec 2019 ISSN: 0975-721X

SECURITY IN MOBILE ADHOC NETWORKS

***Dr Deepak Saxena**

Abstract

This paper discusses about the securing Ad Hoc networks represents a serious challenge. This is due primarily to the open nature of a MANET environment which relies on the air interface as being the medium of transmission of all traffic. In this context, MANETs inherit all vulnerabilities of traditional wireless technologies.

Keywords: Mobile, Network, MANET, Adhoc.

Introduction

A mobile ad hoc network (MANET) is a collection of mobile nodes that can instantly establish a network, whenever they coexist in the same neighborhood without the need of any fixed infrastructure or centralized administration. In a MANET nodes can move around freely and cooperate in relaying packets on behalf of one another. Because mobile nodes have limited transmission range, distant nodes communicate through multi-hop paths.

In addition many other problems arise from the characteristics of MANETs themselves such as resource limitations. As a result, traditional security schemes implemented on wired networks can not be simply imported to a MANET environment. For example, public key encryption algorithm, although safe, includes a significant computational complexity making it hard to implement on mobile nodes with limited processors, memory, and power. As a result, care should be exercised when trying to design a security mechanism suitable for wireless environments where no fixed infrastructure can be referred back to, and hence no way to work around the problem by delegating all the complexity to a fixed and powerful system.

With the ever increasing population in the world, the cyber threat is also growing in frequency and variation. Cyber threats include cybercrime, cyber terrorism, cyber espionage, cyber warfare etc. These threats pose a wide range of risks for economies like identity theft, financial losses, destroyed network infrastructure and breach of confidential information. This paper carries out a comparative assessment of cyber threats in the world's most lucrative targets- the BRICS nations which are emerging economies and at higher risk of cyber attacks. The paper focuses mainly on the factors which makes them vulnerable targets of such attacks as well as on the impact assessment of such attacks on these economies. While the impacts of these threats cannot be over emphasized, recommendations were proposed on how these threats can be minimized if not totally eliminated.[1]

*Professor, INMANTEC, Ghaziabad, UP. Email:deepak.saxena@inmantec.edu

Digital wallets are gaining wide popularity across the globe as a means to make payments, transfer funds and manage loyalty relations as well. It enables the consumer the ease of "paying with your phone". Despite the ease of use and several other benefits and the availability of dozens of applications, the consumer's are still skeptical about its adoption. This consumer vacillation is evidenced by the fact that adoption of truly multi-channel "digital wallets" remains low. This necessitates the need to understand the role of consumer's innovativeness (i.e their propensity to adopt) and the perceived ease of use with regards to digital wallet adoption. The objective of this paper is to evaluate various factors affecting the adoption of digital wallets in India. The paper also tries to measure the impact of demographics on these factors. The study is based on a survey conducted among the people residing in the National Capital Region of Delhi. SPSS AMOS being used for the purpose of analysis. The findings of this paper can help companies and government devise strategies to enhance the use of digital wallets in India so as to inculcate the culture of cashless economy.[2]

Security Aspect of Adhoc Networks

Ad-hoc networks are an emerging area of mobile computing. No fixed infrastructure such as base stations as mobile switching .Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology.

Security Goals

1. **Availability**: Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

2. **Confidentiality**: Ensures certain information is never disclosed to unauthorized entities.

3. **Integrity**: Message being transmitted is never corrupted.

4. **Authentication**: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5. **Non-repudiation**: Ensures that the origin of a Message cannot deny having sent the message.

Security Using Key Management Protocols in Mobile Ad Hoc Network

This point covers the critical issue of securing a Mobile Ad hoc Network (MANET). Such networks exhibit a number of characteristics that make such a task challenging. The major problem in providing security services in such infrastructure less networks is how to manage the cryptographic keys that are needed. In order to design practical and efficient key management systems it is necessary to understand the characteristics of mobile ad hoc networks and why traditional key management systems cannot be used. It provides a summary of those key management solutions that have been proposed in the research literature so far. Secure and efficient key management in mobile ad hoc network has been a challenging task for the researchers due to some properties of ad hoc network like dynamic topologies, use of wireless media, no fixed infrastructure, low-energy constraint devices etc. So far a majority of research works have done to achieve a secure routing infrastructure for ad hoc networks and assumes the existence of an efficient key management scheme. Most of the existing key management schemes are either too inefficient or not appropriate for a dynamic topology and small resource constrained devices. This identifies the security requirements of a mobile ad hoc network and analyses some of the existing key management schemes in terms of security, efficiency and their applicability in ad hoc network. Key management schemes using public key cryptosystems seem unfeasible for ad hoc network due to the fact that nodes in a mobile ad hoc network more often have limited transmission and computational power.

Internet Security and Mobile Computing

Mobile access has opened new vistas for various sectors of society including businesses. The ability that anyone using (virtually) any device could be reached anytime and anywhere presents a tremendous commercial potential. Indeed, the number of mobile applications has seen a exponential growth in the last few years. The Internet has undoubtedly introduced a significant wave of changes. The increased electronic transmission capacity and technology further paves a superhighway towards unrestricted communication networks. To provide interworking, the future systems

have to be based on a universal and widespread network protocol, such as Internet protocol (IP) which is capable of connecting the various wired and Wireless networks. Mobile computing environment supports user mobility, network mobility, bearer mobility, device mobility, session mobility, service mobility and host mobility.

Breaching Information Security

Hacking, cracking, and cyber crimes are hot topics these days regarding information security and will continue to be in near future. When the World Wide Web was mainly used to send e-mail and view remote data, the main concern was amateur hackers devising ways to break into large systems for bragging rights'. Hackers are almost impossible to eliminate. As one group is caught, another replaces them. This thesis will tell how hacking is organised and also about some of the ways hackers use to breach security.

Emerging Trends on Web Security

This thesis describes the use of different web security techniques. Every now and then hackers are challenging web security measures. We describe the security systems. Its components and various issues involved in the design of security systems for world wide web involving web server access control through password authentication.

Hash Racking and Its Impact on Information Security

One of the most important classes of typographic algorithms in current use is the class of cryptographic hash functions. Hashes functions are ubiquitous in today's IT systems and have a wide range of applications in security protocols and schemes, such as providing software integrity, digital signatures, message authentication and password protection. In the Crypto 2004 conference one of the big news was that a fundamental technique in Typography i.e. Message Digest 5 (MD5,) had been cracked. Soon after this event, it was announced that the Secure 1-lash Algorithm (SHA-1) had been cracked. Data assurance has come under scrutiny due to attacks on hashing schemes. This thesis will discuss in detail the broken MD5 and SHA-l, which both are reported to have been cracked, and Wi-Fi investigate any impact. This thesis also shows the implications of these recent attacks, and the possible directions for the development of the theory of hash functions.

Conclusion

Every node in a MANET acts as a router that discovers and maintains routes to other nodes in the network. Efficient routing of packets is a primary MANET challenge. Various protocols have been proposed for efficient routing. However, there are several challenges to ensure routing to MANET as mentioned below:-

All signals go through bandwidth constrained wireless links, which make them more prone to physical security threats than fixed networks.

As the mobile nodes move independently of each other and move in any direction, a security solution with static configuration would not be adequate for frequent changing topology. Decentralized decision making in MANET relies on the co-operative participation of all nodes. The malicious node could block the traffic traversing it, by refusing co-operation thus breaking the co-operative algorithm. More of the nodes rely on batteries or other exhaustible means for their energy. An attacker can cause the replaying of the packets in the network leading to the exhaustion of energy in the nodes.

References

1. Ruchika, Gupta and Agarwal, S.P., (2017). "A Comparative Study of Cyber Threats in Emerging Economies". Globus: An International Journal of Management & IT, 8(2); 24-28, ISSN: 0975-721X.
2. Singh, Gurinder, Kumar, Bhawna and Gupta, Ruchika, (2018). "Role of Consumer's Innovativeness & Perceived Ease of Use to Engender Adoption of Digital Wallets in India". ICACE2018, IEEE Xplore, pp.150-158, **(Scopus Indexed)**.
3. Srivastava, Priyanka, Shukla, Rajendra Kumar, Sharma, Shubham, Khanduja, Dinesh, Gupta, Ruchika and Alrasheedi, Melfi, (2020). "Fuzzy Methodology Approach for Prioritizing Maintenance 4.0 Attributes". ICCAKM 2020, IEEE Xplore **(Scopus Indexed)**.
4. Kumar, Puneet and Gupta, Ruchika, (2008). "Information System's Security by using Matrices and Graphs". Conference proceedings on Information Security and Mobile Computing, ABES Engg College, 62-66.
5. Agarwal, Nidhi and Shiju, P.S., (2018). "A

Study on Content Generation for Internet Usage". International Journal of Advanced Research and Development, 3(2); 1380-1382; doi: 10.5281/zenodo.3764806.

6. Agarwal, Nidhi and Shiju, P.S., (2018). "A Study on CMS with Web Usage Solutions". International Journal of Advance Research and Development, 3(2); 1683-1685; doi: 10.5281/zenodo.3807435.

7. Agarwal, Nidhi and Pundir, Neelam, (2017). "Information and Communication and Its Importance". Ambikeya Journal of Education, 8; 40-42; ISSN: 0975-9735.

8. Agarwal, Nidhi and Kumar, Puneet, (2009). "Role of Information Technology in Education". AICTE Sponsored National Conference on Information Integrity & Supply Chain Management Abstracts Proceeding, Book World Publisher, Dehradun, 18.

9. Agarwal, Nidhi, (2009). "Reflection on the Impact of ICT on Teacher Education". Paradigm Shift in Teacher Education, Vayu Education of India, 5, ISBN: 978-93-80097-12-1.

10. Goel, Agarwal, Nidhi, (2008). "A Global Change in Education through Information Technology and Communication". Enterprises Information Systems & Technology, Mac Millan Advanced Research Series, 124-126; ISBN 10: 0230-635-16-4; ISBN: 13: 978-0230-63516-6.

11. Kapri, Tapan and Kumar, Puneet, (2011). "Web Content Management System". Information and Communication Technology", Excel India Publishers, New Delhi, 8-10.