DESIDOC Bulletin of Information Technology, Vol. 25, No.1, January 2005, pp. 13-18

Wireless Network Security Issues

Ashwani Kush & Ram Kumar

Abstract

In the time span of just a few years, wireless networking has emerged from a novelty to revolution. The speed with which wireless networking has caught on is not surprising owing to large bandwidth and range of several hundred feet. Moreover multiple wireless access points can be easily installed on same network to cover more areas. Our main challenge in design of these networks is their exposure to security attacks. Routing protocols for wireless networks are still an active research area. There is no single standard routing protocol. Therefore we aim to consider common security threats into account to provide guidelines to secure routing protocols. In this paper a study has been carried out for the threats on wireless networks and security goals to be achieved.

1. INTRODUCTION

The advent of wireless networking has raised some very compelling issues. Most important are security issues.[1,2] Other issues can be legal and social. Since their emergence in the 1970s, wireless networks have become increasingly popular in the computing industry. This is particularly true within the past decade which has seen wireless networks being adapted to enable mobility. Wireless networks are emerging fast as latest technology to allow users to access information and services via electronic media, without taking geographic position in account. Mobile hosts and wireless networking hardware are becoming widely available, and extensive work has been done recently in integrating these elements into traditional networks such as the internet. Wireless networks have taken the world by storm. Enterprises and people using computer at home are avoiding the expenses and delays associated with installing wired networks. High speed internet facility is enjoyed by travellers all over the places worldwide. Along with increases in throughput, wireless networks remain unlicensed and affordable. This has further helped their exponential growth in businesses, homes, communities and open spaces. There are currently two variations of mobile wireless networks. The first is known as infrastructured networks, i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. Typical applications of this type of network include office wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure less mobile network, commonly known as an ad-hoc network. A 'mobile adhoc network'[3] is an autonomous system of mobile hosts which are free to move around randomly and organise themselves arbitrarily.

2. NEED OF SECURITY

Over a decade or so there has been tremendous changes in the way people communicate. Description of computing device has changed from PC to communication systems, PDAs, smart phones

and so on. Moreover there are over one billion subscribers using mobile phone technology as opposed to the number of PCs installed. The new computing devices have the capacity to transmit data in its varying forms, not only to similar devices, but also to different devices across a network. Mobile internet and mobile network are reality now. The convergence of technologies has made the devices and the network upon which they operate, more interchangeable than ever before with their overlapping applications. The market is also using latest technology as in E-Commerce which uses B2B (Business to Business), B2C (Business to Consumer), G2G (Government to Government) and G2C (Government to Citizen) all requiring data exchanges. Also some private communication systems like VPN (virtual private network) and VPA (virtual private access) uses a lot of communication between two networks.

According to IDC sources, Global internet commerce is expected to hit US$ 1 trillion by the end of 2004. With so much abundance of networking, it is becoming more and more needful to have a secured transmission and so security has become a major element in both hardware and the application software. It is being argued that, though a high degree of transmission is already in process, the number would be much greater if data security could be guaranteed. To ensure future growth of markets and their applications, a high degree of security is required, due to potentially high commercial value of both the business and private data is being submitted. The need for security arises due to:

- Growth of mobile internet access and applications,
- Individual user requirements, and
- Corporations (business or governmental) who both require internal and external contact and data transfer through remote places.

3. SECURITY ISSUES

Security is an important issue for wireless networks, especially for those security sensitive applications. Many users of data transmission devices (such as laptops, PDAs, PCs, phones, etc.) demand for Protecting data residing within devices, protecting the transmission network, protecting transfer of data, and ensuring proper transfer. One of the goals of current wireless standard was to provide security and privacy that was 'Wired equivalent' and to meet this goal, several security mechanism were provided for confidentiality, authentication, and access control.[4,5,6] Unfortunately all of these can be easily broken.[7,8] Points to consider as security parameters are:

(a) Identity: An essential element in any security system is reliable, robust non-malleable identity.

(b) Access control: Access control is the constraint that limits those who can utilize system resources. Two approaches are used, one is called 'access control list (ACL)' and other as 'closed network'.

(c) Authentication: It ensures that communication from one node to other is genuine. Only legitimate users can access the system and services. Two used systems are 'open system' and 'shared key'.

(d) Availability: Availability ensures the service offered by node will be available to its users when expected, in spite of attacks. Also only legitimate users can access data anytime.

(e) Integrity: It protects nodes from maliciously altered messages. The receiver wants to be sure that the source is genuine. It assures the data, system or platform has not been tampered with.

(f) Non repudiation: It ensures that the origin of the message cannot deny having sent the message.

(g) Confidentiality: It ensures that certain information is never disclosed to unauthorized entities. Personal or sensitive data is protected.

4. ATTACKS

There are two types of attacks toward security protocols: (a) External and (b) Internal.

4.1 External Attacks

External attacks can be passive and active. Passive attacks are unauthorized interruption of the routing packets and active attack is from outside sources to degrade or damage message flow between nodes.

4.2 Internal Attacks

A compromised node is categorized as internal attack. This is most severe threat for adhoc networks. This may broadcast wrong routing information to other nodes

The inheritance feature of wireless networks poses opportunities for attacks from passive eavesdropping to active impersonations, and message distortion. As is often the case, proper security may not be built in at the beginning.

Active external attacks on the wireless routing protocol can be described as denial-of-service attacks, complete break in communication between nodes or degrading. One type of attack involves insertion of extraneous packets into the network which in turn causes congestion. Another attack involves intercepting a routing packet, modifying its contents, and sending it back into the network or to replay it back to the network at different times, introducing outdated routing information to the nodes. One of the attack is called 'man in the middle' means intervention of a third party within communication path without knowledge of source and receiver. Another is 'woman in the middle' means one of the parties (source or receiver) is replaced by attacker.

5. SECURITY MODELS

5.1 Virtual Private Network (VPN)

This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (internet protocol) data grams. Software are available to implement VPNs on just about every platform. Authentication depends upon three factors which are password, fingerprints, and a security token. Using two factors is desirable and using all three is most secured. VPN only supports IP so it cannot be solution for all environments.

5.2 Encryption

Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plaintext (or text) and a message used to conceal original message is called ciphertext (or Cipher). The process of changing plaintext into ciphertext is called encryption and the reverse process is called decryption. There are many algorithm available for these processes. Some of them are Data Encryption Standard (DES),[9] International Data Encryption Algorithm (IDEA)[9] and Public Key Algorithm (RSA).[10] These are based on key based algorithms. There is one popular key algorithm known as Digital Signature algorithm.[11] In Digital signature, signer encrypts the message with key, this is sent to recipient, the message is then decrypted with sender's public key. In case of ad hoc networks this may not be the best method as it uses a lot of space and is also slow.

5.2.1 One Way Hash Function

There is another algorithm called 'One Way Hash Function'.[12] It is like checksum of a block of text and is secure because it is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces an affixed size tag as output. This algorithm can be combined with encryption to provide an efficient and effective digital signature.

5.2.2 Digital Signature

External attacks can be checked using confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital signatures and one way functions can be applied.[13] Perlman[14] used complex robustness to protect routing data from compromised nodes. It is ability to continue correct operation in presence of arbitrary nodes with complex failures.

5.3 Mobile Security Solutions

In mobile security, the solutions which are in use are: PKI system (Cryptographic Key System), Silicon-based Security (as hardware security), SIM Card Security, UICC (Universal Integrated Circuit Card), RFID (Radio Frequency Identification), Secure Mobile media on mobile devices, WAP portals, Dual slot phone, Blue tooth, and Biometrics. Authentication can be done using biometric security, external tokens, cryptographic co-processors, firewalls and software security programs.

Most security models only secure one of the four elements, rather than all which are: secure authentication, confidentiality-privacy, integrity, and data availability .

Security lapses lead to collection, exploitation, falsification, and destruction of data or transactions.

6. RELATED WORK

6.1 Secure Routing

Secure routing in networks such as internet has been very widely studied.[15-20] These routing protocols proposed, cope well with dynamically changing topology. However none of them, to the best of our knowledge, have mechanisms to guard against malicious attacks. To deal with external attacks, standard schemes like digital signatures are used to protect authenticity and integrity. Kumar[16] considers problem of compromised route as a hard problem, but suggests no solution to it. Also Sirios and Kent[19] gave idea of one-way hash function with windowed sequence number for data integrity and also use of digital signatures. Perlman[14] gives idea of how to protect routing information from compromised routers in the context of Byzantine robustness. It only analyses theoretical feasibility under some assumptions. Murphy and Garcia,[17] Sirios and Kent[19] and Smith and Murphy[20] gave only partial solutions to the problem. They give the basic idea to detect inconsistency using redundant information and to isolate compromised routers. Smith and Murphy also gave the idea to secure distance vector routing protocol for ad hoc networks, the method suggested is to add extra information of a predecessor in path to destination in the routing table. They suggest using this information, correctness of path can be verified by path traversal technique. Though it adds cost factor and is mostly avoided.

6.2 Security in Wireless Networks

An authentication architecture for mobile ad hoc networks is proposed by Jacobs and Corson.[21] This architecture can accommodate different schemes. Another authentication architectures include X.509 standard,[22] Kerberos.[23] These are based on certificate authority (CA) but these are not very suitable for ad hoc networks because of infrastructure less support by ad hoc networks, dynamic topologies, frequent route changes. Another model, a slight variation of these models called Hierarchical exist but it also does not address issues like robustness and service availability.

PGP trust model follows a 'web of trust' authentication model. This also is not successful, because it is difficult for each node to maintain a long list of trusted friends.

6.3 Threshold Secret Sharing

Threshold secret sharing serves as primitive in many security function areas in literature of security functions. Much literature is available in this area[25-29] Threshold sharing leads to need of defending against compromised servers. Fox and Gribble[30] propose a Kerberos-based authentication. Zhou and Haas[31] proposed "securing ad hoc networks" applies the threshold secret sharing and proactive secret share update schemes in a fixed group of special nodes. Another paper from Luo, Zerfos Kong, Zhang from UCLA, Los Angeles, CA proposed a "self securing ad hoc wireless network" which claims the model to be almost perfect in assumed conditions. They highlight the features as: system does not expose to any single point of compromise, single point of denial of service attack, or single point of failure. The model sales to large network size and is robust against wireless channel errors. Though the model handles only node

authentication but can be applied to user authentication as well. It uses cryptographic primitives RSA .

6.4 Complex Robustness

Perlman [14] used complex robustness to protect routing data from compromised nodes. It has ability to continue correct operation in presence of arbitrary nodes with complex failures.

6.5 Distributed Key Management

It involves designation of a set of 'Trustworthy' nodes that share sections of the public key of the management system. Each trusted node keeps a record of all public keys in the network. The number of nodes needed to generate a valid signature is less than the total number of trusted nodes. The solution is called 'Threshold Cryptography'.

7. CONCLUSION

As wireless networks are becoming more sophisticated and also offering more applications, number of security sensitive areas will appear depending on number of interfaces. There are a number of security efforts underway currently from both manufacturers and users, but still none of the individual security feature can encompass the meaning of security as a whole. Security measures should be categorized as: Technical, logical, organizational, procedural and physical by tactics which are preventive, detective, repressive and corrective. Active attacks can be checked via authentication and integrity assurance services. External attacks can be checked via confidentiality or routing information and encryption. Also digital signatures or one way function can be solutions. The security services required to combat these active attacks are authentication and integrity assurance. Authentication of routing messages allows nodes to disregard any information that does not come from a trusted source. The integrity of a message will avoid a node from using any information that has been modified in transit. External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital Signatures and One Way Hash Functions can be applied.

What is needed is a variety of security elements with external security tokens and embedded features in IC to create secured platforms.

REFERENCES

1. Stajano, F.; & Anderson R. The resurrecting duckling: Security issues for adhoc wireless networks. www.cl.cam.ac.uk/~fms27/duckling/duckling.html, April 1, 2000.
2. Smith, B.R.; & Garcia-Luna-Aceves, J.J. Securing the border gateway routing protocol. Proceedings of Global Internet '96, November 1996.
3. National Science Foundation. Research priorities in wireless and mobile networking. www.cise.nsf.gov.
4. Arbaugh, W.A. An inductive plaintext attack against IEEE 802.11. Working Group, 2001.
5. Arbaugh, W.A.; & Shankar, N. Your wireless network has no clothes. *In* First International Conference on Wireless LANs, Singapore, 2001, pp. 131-44.
6. Borisov, N.; & Wagner, D. Intercepting mobile communications. *In* Proceedings of International Conference on Mobile Computing and Networking, July 2001, pp. 180-89.
7. Fluhere, S.; & Shamir, A. Weakness in key schedule algorithm. *In* Proceedings of Workshop on Selected Areas of Cryptography, 2001.
8. Frankel, S. Demystifying the Ipsec puzzle. Artech House, Boston MA, 2001.
9. Stallings, W. Data and computer communications. Prentice-Hall, New Jersey, 1997. pp. 623-64.
10. Gennaro, R.; Jarecki, S.; Krawczyk, H.; & Rabin, T. Robust and efficient sharing of RSA functions. Advances in Cryptology Crypto '96, Springer-Verlag, Berlin, 1996, pp.157-72.

11. Chen, D.; Perez, A.; Sasanus, S.; & Verma, S. Encryption: Technical and policy issues. http://128.138.105.73/capstoneTest/Proceedings.asp, Fall 1999.
12. Savard, J. One-way hash functions: A cryptographic compendium. http://fn2.freenet.edmonton.ab.ca/~jsavard/mi0605.htm, April 1, 2000.
13. Smith, B.R.; Murphy, S.; & Garcia-Luna-Aceves, J.J. Securing distance-vector routing protocols. Proc. Symposium Network and Dist. System Security, Los Alamitos, CA, Feb. 1997, pp. 85-92.
14. Perlman, R. Network layer protocols with byzantine robustness. Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1988. PhD thesis,
15. Rover, E.M.; & Toh, C.K. A review of current routing protocols for ad hoc networks. *IEEE Communications,* 1999, **6**, 46-55.
16. Hauser, R.; Przygienda, T.; & Tsudik, G. Lowering security overhead in link state routing. *Computer Networks,* April 1999, **31**(8), 885-94.
17. Kumar, B. Integration of security in network routing protocols. *SIGSAC Reviews,* 1993, **11**(2),18-25.
18. Murphy, S. & Garcia-Luna-Aceves, J.J. An efficient routing algorithm for mobile wireless networks. *MONET,* October 1996, **1**(2), 183-97.
19. Sirois, K.E.; & Kent, S.T. Securing the Nimrod routing architecture. *In* Proceedings of Symposium on Network and Distributed System Security, Los Alamitos, CA, February 1997. The Internet Society, IEEE Computer Society Press. pp. 74-84.
20. Smith, B.R.; Murphy, S.; & Garcia-Luna-Aceves, J.J. Securing distance-vector routing protocols. *In* Proceedings of Symposium on Network and Distributed System Security, Los Alamitos, CA, February 1997. The Internet Society, IEEE Computer Society Press. pp. 85-92.
21. Jacobs, S.; & Corson, M.S. MANET authentication architecture. Internet Draft (draft-jacobs-imepauth-arch-01.txt), February 1999.
22. Aresenault, A., & Turner, S. Internet X.509 public key infrastructure. draft-ietf-pkix-roadmap-06.txt, 2000.
23. Kohl, J., & Neuman, B. The Kerberos network authentication service (ver 5). RFC-1510.
24. Perlman, B. An overview of PKI trust models. *IEEE Network,* 1999, **13**(6), 38-43.
25. Gong, L. Increasing availability and security of an authentication service. *IEEE Journal on Selected Areas in Communications*, June 1993, **11**(5).
26. Frankel, Y.; Gemmel, P.; & MacKenzie, P. Proactive RSA. *CRYPTO,* 1997.
27. Frankel, Y.; Gemmel, P.; & MacKenzie, P. Optimal resilience proactive public–key cryptosystems. FOCS'97, 1997.
28. Gennaro, R.; Jarecki, S.; & Rabin, T. Robust and efficient sharing of RSA functions. *Journal of Cryptology*, 1996.
29. Frankel, Y.; & Desmedt, Y. Parallel reliable threshold multi signature. Technical Report TR-92-04-02, Dept of EECS, University of Wisconsin-Milwaukee, 1992.
30. Fox, A.; & Gribble, S. Security on the move: Indirect authentication using Kerberos. *ACM MOBICOM*, 1996.
31. Zhou, L.; & Haas, Z.J. Securing ad hoc networks. *IEEE Networks*, 1999, **13**(6), 24-30.

Contributors: **Sh. Ashwani Kush**, Department of Computer Science, University College, Kurukshetra, Kurukshetra, 132119. e-mail: akush20@rediffmail.com

Sh. Ram Kumar, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, 132119. e-mail: rkckuk@rediffmail.com