International Indexed, Referred Research Journal, ISSN-2250-2599, January,2013

Research Paper - Computer Science

Security Issues in Wireless Networks

*** Patil S. S.**

Security issues in wireless networks can be considered from three aspects: security requirements, security attacks and security mechanisms. Various security mechanisms are designed to fulfill security requirements so as to counter against different security attacks. Due to characteristics and constraints of wireless networks, wireless networks are facing more security threats than wired counterparts. In this section, we discuss these three aspects of security issues for wireless networks in detail, respectively.

Security Requirements :

In traditional networks, authentication, confidentiality and integrity are the three fundamental security requirements studied for tens of years in research. These requirements are also basic research objectives in wireless environments. Authentication means that a communication partner can be unambiguously identified during the communication. Sometimes only unilateral authentication is enough for secure communication, while mutual authentication is desired to avoid attacks in most cases. Various authentication protocols are employed to provide mutual authentication for communication networks. Confidentiality means that the exchanged information during the communication is not disclosed to unauthorized parties. Encryption, implemented by stream ciphers and block ciphers, is used to achieve confidentiality. Integrity ensures consistency of data and detecting unauthorized creation, alteration, or destruction of data.

This can be achieved by using message authentication code (MAC), or message integrity code (MIC). Non-repudiation sometimes is also mentioned as a basic security requirement in some applications like billing. This requirement prevents either the sender or the receiver from denying a transmitted message, and digital signature is usually used to provide non-repudiation as well as integrity. In wireless environments, we also consider the following security requirements. Availability ensures legitimate parties are not unduly denied access to resources and services of host networks. This requirement is very important as a network is meaningless if it cannot provide services. To assure availability, security solutions should offer resistance to denial-of-service (DoS) attacks, including memory-DoS, computation-DoS and network bandwidth-DoS attacks. Access control requires that only authorized parties can access the wireless network. Fine grained access control, ideally on a per-packet level, should be enforced for wireless networks. Perfect forward secrecy is crucial in that it protects previous session keys and confidential messages against compromising of long term secrets, like private keys, passwords. A new requirement introduced by the unique features wireless networks is anonymity, which requires the identity of the mobile user should be protected from the network it gains access to. This requirement implies user location privacy and unlinkability between two communications, and protects the user's motion pattern from being disclosed.

At the end, an important requirement on security schemes for wireless networks is efficiency. The security solution should be efficient in both computation and communications as mobile devices are usually resource-constrained and the bandwidth is limited in wireless networks.

Security Attacks :

Security research in traditional networks has identifies various attacks against communicating parties, and such attacks can be also applied against wireless networks. Generally, these attacks can be divided into two major types: passive attacks and active attacks. Passive attacks do not involve any message alteration, and refer to eavesdropping or traffic analysis. In contrast to passive attacks, active attacks involve some modification or creation of messages during communication. Passive attacks are hard to detect, but they are not as dangerous as active attacks because they do not affect execution of security protocols. Compared to passive attacks, active attacks are much more dangerous and difficult to defend since their active intervention causes much more problems for security protocols. Fortunately, they can be detected by legitimate communication parties.

Common passive attacks mainly include eavesdropping and traffic analysis. Active attacks, however, can be classified into the following categories. Masquerade attacks refer to an illegitimate entity pretending to be an authorized entity. While replay attacks refer to

retransmission of previously captured messages which may result in unauthorized effect. Message alteration attacks are to modify messages from an authorized party to produce unauthorized effect. While Denial of Service (DoS) attacks aim to degrade performance of networks and prevent normal access to network services and resources. What has been discussed is a general classification of attacks in communication networks, and some attacks may employ much more complex analysis and techniques. For instance, the well-known man-in-the-middle attack is a complex form of masquerade attack; several parties can also collude to compromise secrets of other parties, which is referred to as the collude attack.

Threat of these attacks has been intensified due to the nature of wireless medium. Attacks against wireless networks can be launched without physical connection to the target networks. For example, attackers can easily eavesdrop or analyze traffic in wireless networks within radio transmission range using a suitable transceiver. Also access to wireless networks is open to attackers as no physical boundary exists. And denial of service attacks are more effective in wireless networks since wireless networks are resource-constrained. Moreover, privacy information like identity and location in wireless networks can be the target of attacks.

REFERENCE

* Mishra and W. A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard," Technical Report CS-TR-4328, UMIACS-TR-2002-10, University of Maryland, February 2002. * C. Boyd and D.-G. Park, "Public Key Protocols for Wireless Communications," in Proceedings of the 1998 Internatinal Conference on Information Security and Cryptology (ICISC'98), 1998. * IEEE Standard 802.11-2007, Institute of Electrical and Electronics Engineers, "Standard for Local and metropolitan area networks - specific requirements - part 11: Wireless LAN Medium Access Control and Physical Layer specifications", 2007. * Theodore S. Rappaport. Wireless Communications:Principles & Practice. Prentice Hall, February 2002.