Journal on Information Sciences and Computing, Vol.1, No.1, December 2007

Wireless Security

P.DANANJAYAN
Professor & Head
Dept. of Electronics & Communication Engg.
Pondicherry Engineering College, Pondicherry-605014
pdananjayan@rediffmail.com

Wireless access to the Internet is becoming pervasive with diverse mobile devices being able to access the Internet in recent times. Current deployment is small and the security risks are low as of today in these emerging technologies. However widely varying features and capability of wireless communication devices introduce several security concerns. But security involving communications and networks is not as simple as it might first appear to the novice.

There are three kinds of people who disrupt the security in our network system. They are attackers, hackers and crackers. Attackers steal (or) disrupt the company assets. Attacks are divided into two types such as passive attacks and active attacks. Passive attack attempts to learn or make use of information from the system but does not affect system resources. But, Active attack attempts to alter system resources or affect their operation .The hackers on the other hand will have a deep understanding of the network and in turn affect the network. Crackers understand both information and system and in turn illegally or un ethically penetrate the system.

But security is of paramount concern in wireless networks because they are more vulnerable to malicious exploits than a wired (traditional) network.(i.e)Firstly, the use of wireless links renders the network susceptible to attacks ranging from passive eaves dropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attack on a wireless network can come from all directions and target at any node. Damages can include leaking secret information, message contamination and node impersonation.

Second, mobile nodes are autonomous units that are capable of roaming independently. This means that nodes with inadequate protection are receptive to being captured, compromised and hijacked. Since tracking down a particular node in large scale wireless networks may not be easily done, attacks by a compromised node from with in a network are far more damaging and much harder to detect. Therefore, mobile node and the infrastructure must be prepared to operate in a mode that trusts no peer.

Third, Decision making in mobile computing environment is sometimes decentralized and some wireless network algorithms relay on cooperative participation of all nodes and the infrastructure. The lack of centralized authority means that adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms.

Generally, security deals with the protection of the network against any damage and hides the information when it flows through it. The requirements seem to be straightforward; indeed most of the major requirements for security services can be given self explanatory one world labels: confidentiality, authenticity, integrity and freshness. But the mechanism used to meet those requirements can be quite complex and understanding them may involve rather subtle reasoning. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. Security mechanisms usually involve more than a particular algorithm or protocol. They usually also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution and protection of that secret information. There is also a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. There are two types of security mechanisms such as information security and network security.

Information security can be implemented by different techniques such as cryptographic algorithms and access control techniques. Cryptographic algorithms can be categorized into three, based on the number of keys that are employed for the encryption and decryption. They are conventional cryptography techniques, public key cryptography techniques and Hash algorithms. Hash functions use a mathematical transformation to irreversibly “encrypt” functions.

Introduction of distributed systems, set of networks and communication facilities for carrying data between terminal user - computer and between computer - computer affects the security in the network. So network security is essential to secure the Information (E-mail security), Protocols (IP security) and Web (Web security) in the wireless systems.