International Journal of IT & Knowledge Management (ISSN: 0973-4414)
July-Dec 2008, Vol 1, Number-2, pp 600-604

Communication Cryptography for Wireless Network

Chhattar Singh Lamba
Research Scholar, Jai Narain Vyas University Jodhpur
kunjean_lamba@yahoo.com

Abstract: In today's information age, wireless communications play an important role, which is contributed to the growth of technologies. Wireless Communication Security is increasing in importance as a result of the use of electronic communications in more and more business activities. Therefore, a mechanism is needed to assure the security and privacy of information that is sent over the electronic wireless communications media is in need. Whether the communications media is wired or wireless, both can be not protected from unauthorized reception or interception of transmission. The, method of transforming the original information into the unreadable format is called encryption and decryption of information. The study of encryption and decryption is known as Cryptography. Cryptography is the only practical means to provide security services in many applications. Cryptography or communication by using secret code was used by the Egyptians some 4000 years ago. The secure transport of messages was the concern of many early civilizations. However, the science of cryptography was initiated by Arabs since 600s.Cryptography becomes vital in the twentieth century where it played a crucial role in the World War I and 11. This paper focuses on the analysis of the two types of key cryptography exists, based on the availability of the key publicly:
Symmetric-key Encipherment and Asymmetric- Key Encipherment. In Symmetric-key Encipherment uses a single secret key for both encryption and decryption. Encryption/decryption can be thought of as electronic locking. In Asymmetric Key Encipherment we have the same situation as the Symmetric, with a few exceptions. First there are two keys instead of one: one public and one is private key. The most famous example of this type of cryptography is the Data Encryption Standard (DES).

The most famous example Symmetric-key Encipherment is the Data Encryption Standard (DES). Where as the common example of Asymmetric-key is RSA (Rivest, Shamir and Adleman)

1. Introduction

Any security attack to a wireless system will involve an attack at one or more of the following six levels namely: Network, Transport, Data Link, Transmission, Operating Systems and Applications. We will discuss the attacks in each of these layers and describe the security mechanisms, which need to be put in place to minimize the success rate of intrusion and unauthorized access at each of these levels. For a long time, the wireless industry has responded to security threats on an as needed basis. When vulnerability is discovered, an attempt is made to patch or fix it. This approach leaves systems at the mercy of the next wireless security attack.

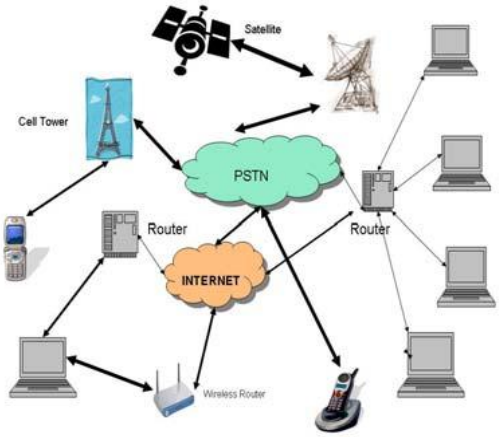

Fig. 1: Typical Data Communications Network

It is now recognized that a comprehensive and principled approach to the solution of wireless security and privacy is necessary. Guttman has proposed wireless authentication tests and disjoint wireless encryption as a possible solution. H. Mantel and A. Sabelfeld have suggested a unified approach to the security of wireless distributed and multi-threaded programs running on portable wireless operating systems. There are many other approaches being suggested. In this paper, a layered approach is proposed since attacks penetrate the system at specific layers of a wireless network before proceeding to other layers. It is instructive to examine the evolution of wireless networks over time in order to better grasp the security implication.

Short Messaging Service (SMS): Transfer of text messages between cell phones.

High-Speed Circuit-Switched Data (HSCSD): This was the first attempt at providing data at high speeds data over GSM, with speeds of up to 115 kbps. This technique cannot support large bursts of data. HSCSD was not widely implemented and GPRS became a more popular technique instead.

General Packet Radio Service (GPRS): This technique can support large burst data transfers. In order to support this, two new elements were added to existing networks namely: (i) Security and Access Control Service and (ii) gateway support for services interconnection.

Enhanced Data Rates for GSM Evolution (EDGE): Standard GSM uses GMSK modulation. Edge uses 8-PSK modulation. GPRS and EDGE combined provide data rates of up to 384 kbps.

Cellular Digital Packet Data (CDPD): CDPD is a packet based data service. CDPD is able to detect idle voice channels and uses them to transfer data traffic without affecting voice communications

Plain text---encryption----→CIPHER TEXT-------DECRYPTION------→Plain text

Figure 2, Asymmetric Encryption

2. THE ROLE OF CRYPTOGRAPHY IN COMMUNICATIONS

Security of communications was historically the concern of military and government interests. However, the importance of communications security in the commercial sector has been increasing in recent years and will continue to do so in the future. This is because of the ever greater reliance on electronic communications, particularly data communications, for the running of commerce and industry, which makes valuable commercial resources vulnerable to a variety of threats which have not previously been of concern. Provision of security services can be expensive, particularly if provided on an ***ad*** *hoc* basis for each application separately. An important way to alleviate this cost is through the development of standard security solutions, which can include standardized secure protocols and procedures, as well as cryptographic algorithms.

3. LAYERED ATTACKS ON WIRELESS SYSTEMS

A wireless network consists of two or more wireless devices connected in some topology using a set of communications protocols over one or more transmission channels. The wireless topology describes the way in which the wireless devices are connected. Typically there a transmitting cellular device communicates with a cellular or other radio based tower, which acts as a base station, routing the communication to a receiving device, which may be another cellular device. This may be a peer-to-peer, star, ring, circular or other topology.

The wireless communications protocol is a set of rules by which the devices send and receive data, execute programs and share resources over the network. The transmission channels maybe cellular channels, microwave or infrared among others, but this could be looped into fixed wire line channels such as coaxial cable, fiber optics or twisted wire pair. In each case, modern systems use wireless data packets to transmit the data from the source node to the destination node via one or more intermediate wireless nodes (routers, gateways and bridges). There are several protocols used in the transmission of data packets from the source to the destination. The most widely used protocol is TCP/IP, which has four layers in its Protocol Stack suite.

4. WIRELESS SECURITY AND ATTACK VULNERABILITIES

The Evolution of Cellular networks into fully IP based systems poses significantly more security problems than in fixed wire networks. There are at least 10 areas of vulnerabilities which need to be carefully examined in 3G/4G networks namely: device security, authentication, integrity, confidentiality, access control, mobile operating systems security, mobile web services, content downloading, viruses and undesired detection of location. Each of these vulnerabilities while not new, pose new challenges in the more sophisticated 3G/4G wireless architecture.

If a device is lost or stolen, sensitive information such as emails, documents and phone numbers can be compromised. In the 4G environment, the portable device may contain or access as much information as can be accessed via the internet making important data such as credit card information, social security numbers and other sensitive and private information readily available to whoever gains access to the device.

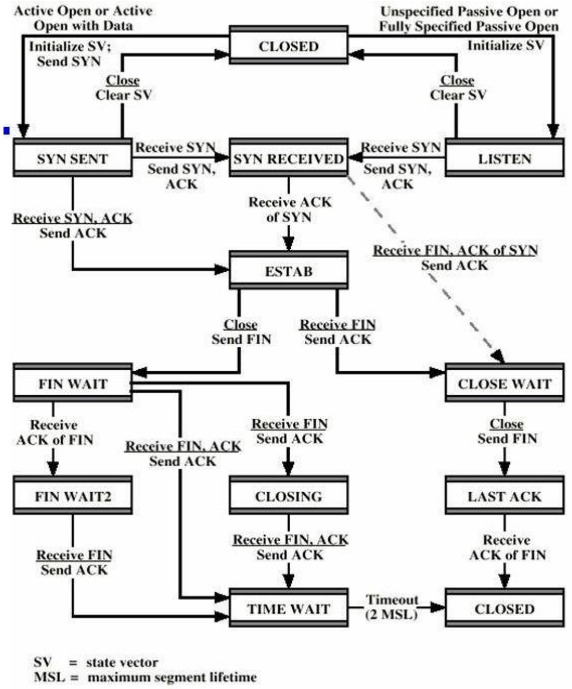

Fig:- 3 Flow Diagram depicting the three-way TCP Protocol Hijack.

4.1 TCP Connection Hijack

An attack host Y allows normal authentication to proceed between two hosts X and Z, and then seizes control of the connection. This is known as a TCP Connection Hijack or a Man-in-the-Middle attack. One way to do this is during the TCP three-way handshake; the other is in the middle of an established connection. The attacking host Y will normally listen in on the communication between X and Z, waiting for the two hosts to de-synchronize. De-synchronization occurs because other intermediate nodes in the channel may be slow. Connection hijacking exploits the "desynchronized state" in TCP communication and injects forged packets with the correct sequence numbers. These forged packets can then be used to modify the contents of the communication and/or add additional commands, which enable the attacker to compromise hosts X and Z. It can be very difficult to determine if there is a connection hijack in progress. One way to minimize the risk of hijacks is to implement additional secret handshakes between two secure hosts

5. SECURITY ATTACKS AT THE WIRELESS NETWORK LAYER

5.1 IP Spoofing Attack

An attacking host A sends messages to a victim host B with an IP address for host C (not its own IP address) indicating that the message is coming from trusted host C to gain un-authorized access to host B. The attacking host A first uses a variety of techniques to find the IP address of a trusted host C. This can be accomplished by sending PING messages to C. Once a trusted host IP has been found, attack host A modifies its packet headers so that it appears that the packets are coming from host C. Attack host A now gains unauthorized access to, and control, of services in host B. A possible solution to IP Spoofing is to have additional secret encryption and access rules between host B and C, which are independent of the packet header address. Fig. 4 below shows the IP addresses and subnet mask addresses for hosts A, B and C.

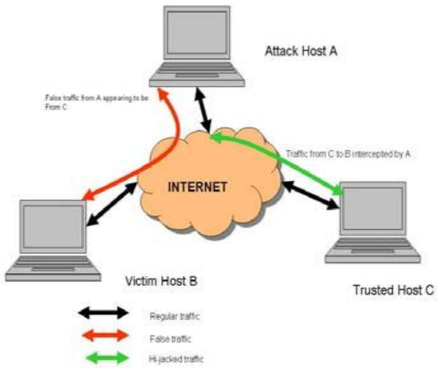

Fig. 4**:** Spoof Attack in progress

5.2 Routing Information Table Protocol (RIP) Attacks

Routing Information Tables are used to determine the intermediate nodes through which packets travel before reaching the final destination. Routing tables have become increasingly sophisticated and in addition to containing information such as the shortest paths, the recent speeds of transmission and congestion, may also include advertising information in certain cases. Routing Information Table Protocols have no built in authentication, and the information provided in a Routing Information Table packet is often used without further verification. Host X forges a RIP packet, claiming host X has the fastest path out of the network, resulting in host X gaining unauthorized access to packets routed through it wherefrom they could be modified or read before further transmission.

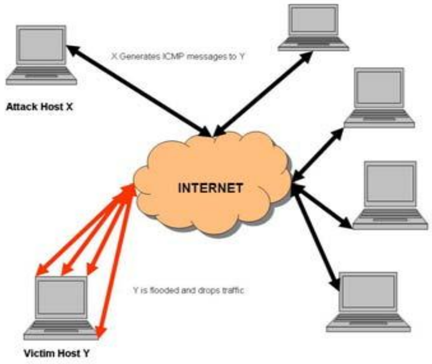
Attack Host X
X Generates ICMP messages to Y
INTERNET
Y is flooded and drops traffic
Victim Host Y

Fig. 5: How Attack host X can flood a Victim Host Y using ICMP messages.

Some others are: -

5.3 ICMP Attacks

5.4 Packet Sniffing Attacks

5.5 Manipulated IP Packet Attack

6. Security Risks in communications,

In recent years, more and more businesses make use of communication networks. Share potential information and therefore sensitive data is located in communications network transmissions that are connected all over the world**.** This commitment to data communication has increased the vulnerability of organization assets. Computer fraud is becoming one of the most popular crimes in our days. Since a network without security mechanisms is like an office building with open doors, the network owner has to make sure to lock those doors and give keys only to those people whom he wants to share the information with. For many people, communications security just means preventing unauthorized access, such as preventing a hacker from breaching into a network. Security is more than that.

7. Discussions and Conclusions

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well- documented because they are also well-tested and well-studied! In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys. The basic concepts, characteristics, and goals of various cryptographic have been discussed.

The study and analysis of Security mechanisms and attacks at the Transport and Network Layers of the TCP/IP protocol enables us to understand the dangers that lay hidden in a computer communications network. Many computer systems remain vulnerable to attacks because computer systems administrators and users are unaware of the loopholes in the underlying technology. It is extremely important that Computer Wireless Security is a serious issue and needs to be addressed at the transport, network, data link, operating system and application layers. An approach in which each layer can guarantee a certain measurable level of security and privacy is necessary to solving the multi-faceted information security and privacy problem.

8. References

[1]. www.cryptogram.org.

[2]. www.crypto.com.

[3]. Cryptography and network security by Behrouz A.Forouzan.

[4]. Vajda, *Extraction of random bits for cryptographic purposes*, Tatra Mountains Mathematical Publications, 2002, vol. 25,

[5]. Ferguson, N. and B. Schneier, *Proclicol Cryptography*. New York John Wiley & Sons, 2003.

[6]. Bauer, F.L. *Decrypted Secrets: Methods and* D.E.R. Denning, *Cryptography and Data Security*

[7]. J. Seberry and J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice-Hall, 1989.

[8]. D. R. Stinson, *Cryptography: Theory and Practice*. CRC Press, 1995.

[9]. B. SCHNEIER, *Applied Cryptography &* Wiley, 1994.