International Journal of Advance Research in Science and Engineering
Vol. No.10, Issue No. 03, March 2021
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Aspects of Security Enhancement of Wireless Networks and Mobile Communications Systems

Seema Sinha

Research Scholar, Deptt. of Mathematics

Magadh University, Bodh Gaya

Abstract:

This paper gives a topical overview of wireless network security aspects. Security measures taken depend on the different protocols, standards, techniques and systems available. A brief introduction to security protocols, standards and corresponding technologies is given. The essay will concentrate on 2G, 2.5G, 3G and wireless local area networks. Standards, like WAP, IEEE 802.11, HomeRF, HIPERLAN/2, IPSec and Bluetooth, are included. A local area network, MediaPoli, has been implemented to work as a testbed for new innovations, products and services. The development environment is based on this high-capacity wired/wireless broadband network. Key research areas, actual projects and offered services are discussed. All activities aim at the future information society.

Keywords: security, mobile, wireless, network, testbed

Introduction

The requirements of information security have undergone three major changes in the last decades. The first major change was the introduction of the computer. The need for protecting files and information be-came evident. Collection of tools designed to protect data and to avoid hacker attacks has the generic name *computer security*. The second major change was the introduction of distributed systems, networks and communication facilities for data communication. *Network security* measures are needed to protect data during transmission. The third change is the current, rapid development of wireless networks and mobile communications. *Wireless security* is therefore of high priority today.

Network Security

Cryptography is an essential part of today's information systems. Cryptography is needed for

- reliable authentication
- integrity of information content
- confidentiality
- nonrepudiation

Network security requires active administration. Security policies, standards and administrative proce-dures must be worked out, implemented and followed up.

Software threats (malicious programs) are divided into two categories: those needing a host program, such as trap doors, logic bombs and Trojan horses and those being independent, such as viruses, bacteria and worms. We can also divide these software threats into programs that replicate and those that do not. Rep-licating software is either a program fragment (virus) or an independent program (bacterium, worm). Non-replicating software are fragments of programs that are activated when their host program performs a spe-cific function (Stallings, 1999).

Many network security solutions and (IETF) standards are based on the assumption that the data commu-nication media is wired. Since network security usually is implemented in the protocol stack at the net-work level - as the IPSec standard (IP Security Protocol, 2002) - or at the application level - as the TLS standard (Transport Layer Security, 2002). - no essential security modifications are needed as long as wireless communication is implemented only at the data link level of the network protocol stack. Wireless LANs (WLANs) and the mobility options in such LANs have however required further development of earlier adopted network security solutions. For example, IPSec assumes that IP numbers of communica-tion network nodes are stable (IP Security Protocol, 2002). IP stability can however not be fulfilled for mobile network nodes roaming between access points in a WLAN. Also TLS and applications using TLS cannot be implemented as such for secure applications in a WLAN environment (Blake-Wilson and Nys-trom, 2000) (Price and Elkins, 2000).

Wireless networks have properties that imply different security solutions for wired and wireless networks. These are (Rysavy, 1998):

- They use the same networking protocols but use specialized physical and data link protocols
- They connect to existing networks via access points which provide a bridging function
- They let you stay connected when roaming from one coverage area to another
- They have unique security considerations
- They have specific interoperability requirements
- The require different hardware
- They offer performance that differs from wired LANs

Wireless and mobile communications is rapidly evolving. An overview of security aspects of needed sys-tems, standards and protocols is given in (Hansen, 2000) (A Comparison of Security in HomeRF versus IEEE802.11b, 2001) (Wireless LAN Security, 2001).

Wireless Application Protocol

In the WAP environment, both the network and the WAP servers can be connected to the public Internet, i.e. the WAP stack and the servers are exposed to attacks. Typical threats and protection methods are:

- Viruses and malicious services are possible in the mobile terminal
- The radio interface is protected with standard GSM security methods

- Mobile networks can have unprotected radio links between the base station and the base station controller
- Stored services of the gateway and the server require similar protection as the Internet server.
- Data transmission between the gateway and the server needs protection.

SSL (Secure Socket Layer) is used in the web world to encrypt the data stream between the browser and the web server. In the WAP environment, SSL is used between the web server and the WAP gateway, but a specialized protocol, WTLS (Wireless Transport Layer Security), is needed between the WAP gateway and the WAP device. WTLS is designed to ensure data integrity, privacy and authentication but WTLS does not take into account whether the content is malicious or not.

WTLS is closely the same as the SSL and TLS protocols, but a number of changes has been made to the protocol by the WAP Forum (WAP Forum Releases, 2002). These changes were motivated by the special requirements of the WTLS protocol :

- Both datagram and connection oriented transport layer protocols must be supported,
- The protocol must be able to cope with long round-trip times,
- The bandwidth of some bearers can be very low,
- The processing power of many mobile terminals is quite limited,
- The memory capacity of many mobile terminals is very modest,
- The restrictions on exporting and using cryptography must be considered.

In other words, the designers of WTLS took TLS and tried to add datagram support, optimize the packet size, and select fast algorithms into the algorithm suite.

At the surface, the WTLS looks reasonably good. Most of the text in the WTLS specification has been adopted, word to word, from the TLS specification. However, many of the changes that were made by WAP Forum have led to security problems. SSL and WTLS on their own seem to provide enough security for most applications. But there is a security problem where the two protocols meet, and that is inside the WAP gateway. SSL is not directly compatible with WTLS. The WAP gateway must decrypt the SSL protected data stream coming from the webserver, and then re-encrypt it using WTLS before sending the data to the WAP device. The problem is that the data is unprotected inside the WAP gateway. Figure 1 il-lustrates this problem.

Wireless Local Area Networks

Today the security of wireless LANs is of much concern. Security measures taken are almost identical in the wired and wireless world. Wireless LANs include an additional set of unique security elements. This implies specialized physical and data link protocols.

Any network is subject to substantial security risks and issues. These include issues like threats to the physical security, eavesdropping and attacks from within the network's user community. Three main se-curity issues are defined by the HomeRF Working Group (Chinitz, 2001):

- Data Compromise is any form of disclosure to unintended parties of information
- Unauthorized Access is any means by which an unauthorized party is allowed access to network resources
- Denial of Service is an operation designed to block or disrupt normal activities of a network

Here we include the following standards and protocols: IEEE 801.11, HIPERLAN2, HomeRF, IPSec and Bluetooth.

IEEE 802.11

The standard defines the physical layers and the MAC sublayers. Version IEEE 802.11b defines two spread spectrum technologies: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). The data rate is 1 Mbps or 2 Mbps using frequency hopping and 1, 2, 5.5 or 11 Mbps using direct sequence. The used spectrum is the 2.4 GHz ISM band.

Two authentication schemes are defined: Open System Authentication and Shared Key Authentication. The former lets anyone (requesting the access) be accepted to the network. The later one uses shared key cryptography to authenticate the mobile. A 1024 bit long encrypted random number is sent by the base to the access requesting mobile terminal. After decryption, the number is sent back to the base and if the number is correct the mobile is allowed to connect to the network. The mobiles cannot be distinguished from each other and no key management functions are defined.

Confidentiality and integrity are implemented through the Wired Equivalent Privacy (WEP) protocol. WEP is used at the station-to-station level and does not offer end-to-end security. The RC4 PRNG integ-rity algorithm (What is RS4?, 2000) is used. It is based on a 40 bit secret key *k* and a 24 bit Initialization Vector (IV) is sent with the data. An Integrity Check Vector (ICV) is included to allow integrity check. The WEP protocol proceeds as follows in order to send a message *M* when the sender and the receiver share a secret key *k* (Borisov, Goldberg and Wagner, 2001):

From source to receiver

- *Compute an integrity checksum (Integrity Check Vector ICV) on the message M*
- *Choose an Initialization Vector IV*
- *Generate a key stream (a long sequence of pseudorandom bytes) as a function of the IV and the key k by using the RC4 encryption algorithm.*

HomeRF

HomeRF v2.0 uses the 2.4 GHz ISM band. The data rate is 0.8, 1.6, 5 or 10 Mbps depending on modula-tion scheme. The standard supports up to 127 devices per network. The typical range is home and yard up to 50 m (SIG, 2001).

Shared Wireless Access Protocol (SWAP) is the technology behind HomeRF. SWAP uses FHSS (Fre-quency Hopping Spread Spectrum). The HomeRF standard uses 128-bit

Blowfish encryption. An IV (Ini-tialization vector) of 32 bits (24 bits for 802.11) is used and the time scale for repeated IV is half a year. The standard completely specifies the manner in which IVs are chosen (Nathan, 2001).

All devices use a "shared secret" network ID (NWID). Without NWID, devices are not permitted to communicate. A client device must synchronize its frequency hopping sequence with the access point in order to receive data. This means that the client and the access point must have identical NWIDs. Thus, over the air, data cannot be captured via another HomeRF radio if NWIDs are different. The authentica-tion process is the following one (Chinitz, 2001):

- A node chooses a fixed frequency and listens for a period of time
- Packets are delivered by MAC to higher levels if
  - the NWID of the receiver matches the NWID of the transmitter
  - the transmitter has been directed to teach the NWID, and the receiver has been directed to learn the NWID

Compared to IEEE 802.11b, attacks against HomeRF are orders of magnitude more complex than those required for 802.11b. This is due to the frequency-static nature of 802.11b.

Denial of Service, DoS, (the network is shut down by an attacker) is employed at protocol levels that can-not be protected by encryption. Frequency hopping must be overcome in order to detect the control frames. The attacker first has to determine where in the frequency regime the access point will be at a given point in time. This is possible but much more difficult than for 802.11b, which uses DSSS.

HIPERLAN/2

HIPERLAN (HIgh PERformance LAN) is a family of standards on digital high speed wireless communi-cation in the 5.15 – 5.3 GHz and the 17.1 – 17.3 GHz spectrum. HIPERLAN types 1 and 2, HIPER-ACCESS and HIPERLINK have been proposed. For HIPERLAN/2 the theoretical data rate is 54 Mbps at a range of 30 to 150 m (SIG, 2001).These standards are being developed by the BRAN (Broadband Radio Access Network) project which is a part of ETSI. HIPERLAN/2 has been developed to provide short range wireless access to IP, ATM and UMTS networks. The standard describes a common air interface and the physical layer, i.e. leaves the higher level functions open to the manufacturers.

The HIPERLAN/2 has support for both authentication and encryption (Johnsson, 2000). Security encryp-tion is scalable using a 56 bit (DES) to 168 bit (3DES) algorithm. The Diffie-Hellmann key exchange procedure is used for creation of the encryption key. Encryption protects against eavesdropping and man-in-the-middle attacks. HIPERLAN/2 authentication relies on identifiers: every communicating network node is given a HIPERLAN ID (HID) and a Node ID (NID). These identifiers identify any station and re-stricts the way it can connect to the other nodes. All nodes with the same HID can communicate with each another. Authentication is based on a supporting function, such as a directory service. With authentica-tion, both the access point and the mobile terminal can authenticate each other.

Conclusions

Wireless network security along with a fast technological change is a demanding field. This overview shows that network security in itself must be seen as a whole. The adopted network security policy forms the basis. A proper choice of system(s), protocols, standards and techniques gives the guidelines for a more secure networking. The security levels of current networks must be constantly enhanced to meet the growing security threats. Wired and wireless networks use in principal the same type of basic security methods. This means that security measures taken to ensure the integrity and security of data in the wired local area network environment are also applicable to wireless LANs. Information systems are strongly affected by secure wireless technology.

In the near future we will see a rapid growth of wireless technology, devices and equipment. Security aspects will enhance this change and the affect on information systems will be significant.

References

[1]. A Comparison of Security in HomeRF versus IEEE802.11b. (2001). Retrieved November 1, 2001 from the World Wide Web http://www.homerf.org/data/tech/security_comparison.pdf

[2]. Adoba, B. (2001). IPsec-NAT Compatibility Requirements, Internet Engineering Task Force (IETF), IP Security Protocol (ip-sec) Working Group, Internet Draft. Retrieved October 11, 2001 from the World Wide Web http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-reqts-00.txt

[3]. Blake-Wilson, S., Nystrom, M. (2000). Wireless Extensions to TLS, Internet Engineering Task Force (IETF), Transport Layer Security (tls) Working Group, Internet Draft. Retrieved June 6, 2001 from the World Wide Web http://www.ietf.org/internet-drafts/draft-ietf-tls-wireless-00.txt

[4]. Borisov, N., Goldberg, I., & Wagner, D. (2001). Intercepting Mobile Communications: The Insecurity of 802.11. Retrieved September 21, 2001from the World Wide Web http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[5]. Chinitz, L. (2001). A Comparison of Security in HomeRF versus IEEE802.11b. Home Toys Article. Retrieved June 17, 2001 from the World Wide Web http://www.hometoys.com/htinews/aug01/articles/security/security.htm

[6]. Dornan, A. (2002). Emerging Technology: Wireless Lan Standards. *NetworkMagazine*. Feb 6. Retrieved March 10, 2002 from the World Wide Web http://www.networkmagazine.com/article/NMG20020206S0006

[7]. Hansen, H. (2000). Security of mobile systems from user's point of view. Seminar Report. Retrieved November 1, 2001 from the World Wide Web http://www.hut.fi/~hansen/papers/user-secu.index.html

[8]. Harte, L., Levine, R., & Livingston, G. (1999). *GSM Superphones*. USA: McGraw-Hill.

[9]. How secure is WAP with SSL and WTLS ?. (2000). Retrieved November 20, 2001 from the World Wide Web http://www.123wapinfo.com/faqs/security/index04.ht

[10]. Huttunen, A., Dixon, W., Swander, B., Sierwald, J., Stenberg, M., Kivinen, T., Volpe, V., & DiBurro, L. (2000). IPsec over NAT Justification for UDP Encapsulation, Internet Engineering. Task Force (IETF), IP Security Protocol (ipsec) Working Group, Internet Draft. Retrieved October 11, 2001 from the World Wide Web http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-justification-00.txt