Security of Mobile and Wireless Networks

Kaj J. Grahn
Arcada Polytechnic, Espoo, Finland

Göran Pulkkis
Arcada Polytechnic, Espoo, Finland

Jean-Sebastien Guillard
Ecole Nationale Superiéure d’Electronique, Bordeaux, France

kaj.grahn@arcada.fi goran.pulkkis@arcada.fi jean-sebastien@guillard.as

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 became 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

in data communication (Schneier, 1996) (Stallings, 2000). *Reliable authentication* means that a communication partner can be unambiguously identified. *Integrity of information content* requires, that reliable methods are available to check that transmitted information remains unchanged on the way from the sender to the receiver. *Confidentiality* means that the sender of information can determine who has (have) the right to read the information content. *Nonrepudiation* means that the authenticated information exchange can afterwards be unambiguously proved to have happened. Nonrepudiation is essential in following up adopted agreements and in reliable e-commerce.

Within the fields from e-mail to cellular communications, from web access to digital cash, cryptography is applied. It prevents fraud in electronic commerce and assures validity of financial transactions. It can prove your identity or protect your anonymity. The importance of cryptography and the number of application areas are steadily growing.

Network security requires active administration. Security policies, standards and administrative procedures 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. Replicating 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 specific function (Stallings, 1999).

Many network security solutions and (IETF) standards are based on the assumption that the data communication media is wired. Since network security usually is implemented in the protocol stack at the network 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 communication 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 Nystrom, 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 systems, standards and protocols is given in (Hansen, 2000) (A Comparison of Security in HomeRF versus IEEE802.11b, 2001) (Wireless LAN Security, 2001).

Mobile Systems of Second Generation

Digital 2G systems, such as GSM, PDC, IS-136 TDMA and IS-95 CDMA, use cryptographic methods for authentication and confidentiality. GSM (General System for Mobile communications) is a standard for digital cellular communications. This standard implements security features which ensure (Kesarev, 1997): 1) physical security, 2) data security, 3) user authentication, and 4) user anonymity.

Slow frequency hopping and modulation techniques enhance the physical security. Information sent between a mobile station and the network is encrypted. Further, monitoring signals of the radio interface requires specialized equipment not freely available.

GSM security is based on a shared secret key *Ki* and on a unique number, the International Mobile Subscriber Identity (IMSI). Both are on the user's Subscriber Identity Module (SIM) and in the Authentication Centre (AuC) of the operator. A signal response number (SRES) is calculated by AuC from Ki, IMSI and from a random number challenge (RAND). SRES and RAND are placed in the Home Location Register (HLR). A mobile terminal is authenticated if its calculated SRES is equal to the stored one. The authentication algorithm is called A3, which is a secret algorithm (Harte, Levine and Livingston, 1999).

The encryption algorithm - A5 - is a secret, symmetric stream cipher using a 64-bit key Kc. The key is handled by three Linear Shift Feedback registers (LSFRs). Key Kc used in algorithm A5 is generated by another secret algorithm, A8. This key generating algorithm uses RAND and Ki as input (Harte, Levine and Livingston, 1999).

Anonymity is achieved by using a Temporary Mobile Subscriber Identity (TMSI). This identity is agreed upon after authentication and key generation through an A5-encrypted channel.

Mobile Systems of 2.5 Generation

GPRS (General Packet Radio Service) is announced to be a mobile system of 2.5 generation. GPRS is rather similar to GSM using the same radio access network in packet mode. Packet handling nodes have to be added. Such nodes are SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Node). Other nodes like HLR (Home Location Register) and AuC (Authentication Center) can be reused with minor modifications.

Internet and Intranet access of mobile and portable devices will be major GPRS applications. GPRS will also be a major carrier of WAP (Wireless Application Protocol) applications. Most GPRS terminals will probably also support GMS. The theoretical data rate is more then 100 kbps but most operators will offer data rates between 20 and 40 kbps (SIG, 2001).

Mainly GPRS offers the same security mechanisms as GSM. The same authentication algorithms and also the SIM-card can be used. The cryptographic key is situated in SGSN in contrast to GSM where the key is placed in the base station (SIG, 2001).

Special cryptographic algorithms are used and the length of the used keys is 64 bits. Localization of a mobile station and the use of temporary user identities is supported. Security in the backbone net and between operators is not standardized.

Mobile Systems of Third Generation

Evolving 3G systems, such as UMTS and CDMA2000, will rely on IP-networks, i.e. open networks, which do not separate signaling from user data. This may allow malicious users to gain access to data and/or network resources. An Internet like security architecture will be adopted by the 3G systems. Third generation systems will support roaming with second generation systems. The compatibility between 2G and 3G systems will probably give a lower security level (Steele, Lee and Gold, 2001).

A smart card will be an obligatory personal security module and it is called USIM. Like in GSM, algorithms for authentication and key generation will be on this card.

New security features are added to take account of changes in network architecture and to secure new services offered by 3G. Compared to GSM two major security developments are included (Knight, 2000):

The cryptography used will be strengthened with the introduction of 128-bit keys. A 128-bit cipher key CK and a 128-bit integrity key IK will be established. Information is encrypted between the mobile station and Radio Network Controller node. Encryption relies on the Kasumi algorithm (SIG, 2001).

Mutual authentication will be introduced using cryptographic keys to establish the identity of both user and base station over a connection. Authentication for users passing between different networks will also be protected using a public key cryptographic system. The algorithms are based on Rijndael (SIG, 2001).

Compared to GSM important signaling is also encrypted. A cryptographic sum check is used in both directions. Also signaling between networks will get standardized security solutions. Confidentiality and integrity will be supported.

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 illustrates this problem.

All major WAP product designers develop solutions to this problem, but for now, these solutions create other problems. WAP servers, or webservers with WAP gateway capabilities, provide end-to-end security, if the data stream leaves the content server (the WAP server) already encrypted with WTLS. Figure 2 illustrates this solution. With this solution, the user has to reconfigure his/her WAP device to point to the WAP server which will become the WAP gateway for this session. But this WAP gateway only provides access to this one service, and when the user wants to access his other favorite WAP sites, he/she has to reconfigure his phone again. However, some WAP devices are extremely difficult to reconfigure.

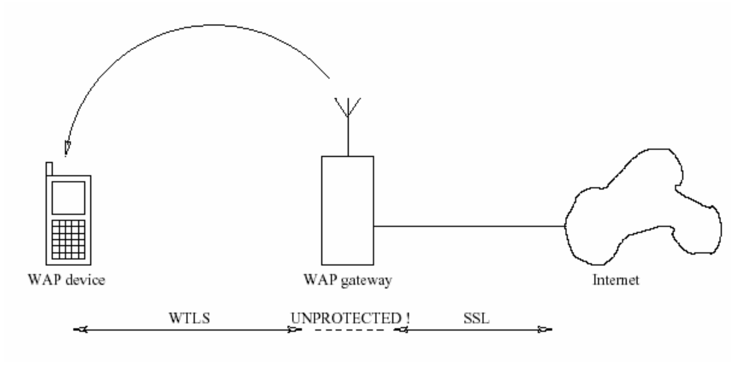

Figure 1. No protection inside the WAP gateway.

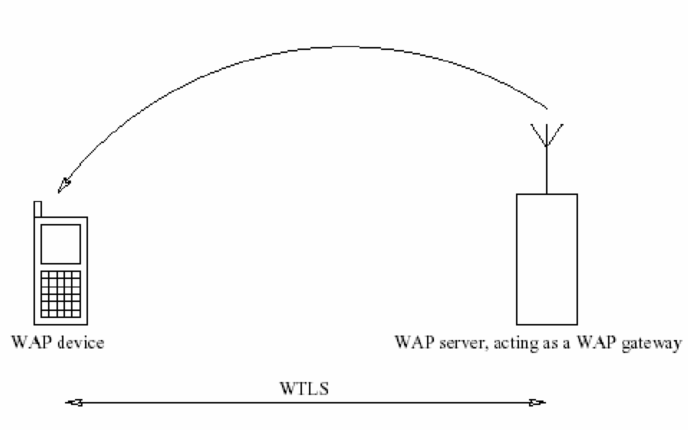

Figure 2. The data stream leaves the content server already encrypted with WTLS.

There is another problem, which stops the user from using other gateways than the one provided by the mobile operator. Many mobile operators place their point-to-point service, where the mobile device dials Internet, and their WAP gateway on the same private IP range network, usually behind a firewall. This firewall is usually set up only to allow the HTTP protocol on the default port (80). The WAP gateway uses this port to receive data from content servers on the Internet. When the WAP device tries to access another WAP gateway on the Internet, the firewall will prevent it either because the firewall says that the IP address of the WAP device is not allowed to route data to Internet, or that it cannot use the ports it requires.

A suggestion is made in (How secure is WAP with SSL and WTLS?, 2000):

“It would be to make WAP gateway accept already WTLS encrypted data streams and simply pass them along to the browser untouched. This would cause the least amount of problems for the consumer. It is easier to upgrade all WAP gateways than all WAP devices. The third party's gateway (for instance the mobile operator) would then just be a relay for the data stream as it is already protected by WTLS by the WAP Server securely located at the company providing the service. In other words, in a model like this the WAP gateway has two modes of operation. In a normal mode it works like WAP gateways work today. The other mode is a passthrough mode where the gateway detects the WTLS stream and simply lets it pass through.”

Figure 3 illustrates this solution.

A number of security flaws and shortcomings in the WAP WTLS protocol have been identified (Saarinen, 1999): a chosen plaintext data recovery attack, a datagram truncation attack, a message forgery attack, and a key-search shortcut for some exportable keys. WTLS seems to need revision.

The security requirements in the WAP environment are similar to those of a company intranet and of web servers. As an example we mention F-Secure Corporation (Securing WAP Environments, 2000) which provides the following WAP security solutions:

- Anti-Virus for WAP Gateways
- SSH for UNIX servers
- VPN+ (Virtual Private Networking when the origin server and the gateway are separated by a potentially hostile network)
- Distributed Firewall (protects servers from network based attacks)
- Policy Manager (security of multiple applications from one central location)

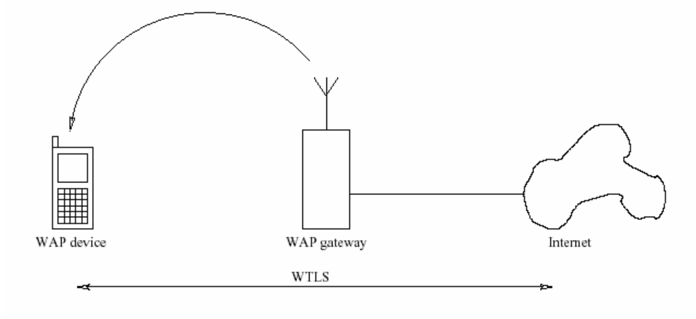

Figure 3. Passthrough mode of a WAP gateway.

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 security 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 integrity 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*
- *Exclusive-or (XOR) the plaintext with the key stream*
- *Transmit the IV and the ciphertext over the radio link*

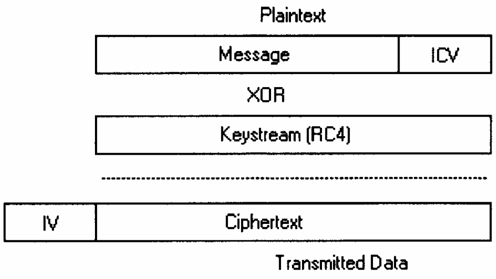

Figure 4. Encrypted WEP frame.

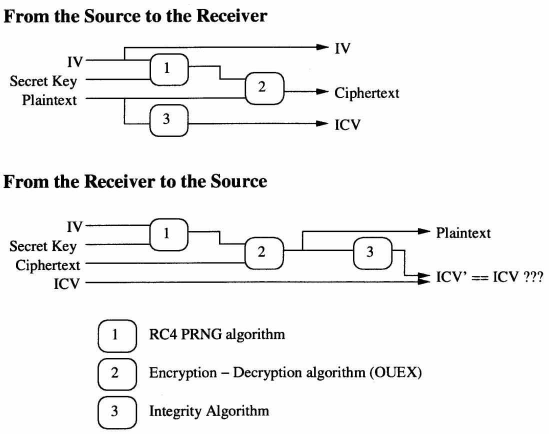

Figure 5. Implementation of WEP.

The encrypted WEP frame and implementation of the WEP algorithm are illustrated in Figures 4 and 5.

Decryption of the WEP frame is a reverse process. The recipient regenerates the key stream and XORs it against the ciphertext to recover the original plaintext. The checksum ICV on the decrypted plaintext is verified and checked that it matches the received checksum ICV, i.e. only frames with a valid checksum will be accepted by the receiver.

Major security flaws in the WEP protocol have been reported (Borisov, Goldberg and Wagner, 2001). These flaws were stemming from misapplication of cryptographic primitives and they lead to attacks that demonstrated WEP failure. In addition the secret key used is only 40 bits long, which can be solved by a brute-force attack in a reasonable amount of time. Every user has the same key which implies that the entire network is compromised if one laptop is stolen (Dornan, 2002).

In newer products, TKIP (Temporal Key Integrity Protocol) has been incorporated. This protocol is informally known as WEP2. TKIP uses 128-bit keys and is fully backward-compatible with WEP. This enables vulnerability to the same type of attacks as for WEP. The protocol also supports Kerberos passwords. This is a potential vulnerability since these passwords can often be guessed through a simple dictionary attack (Dornan, 2002).

The IEEE has more versions on the way. Two of these are 802.11a and 802.11g. Version 802.11a uses OFDM (Orthogonal Frequency Division Multiplexing) and can reach 54 Mbps at the 5 MHz band. The data rate is some misleading because overhead, interference and transmission errors will cut the through-put. Version 802.11a is not compatible with 802.11b and therefore the IEEE developed 802.11g to get around this problem. Versions 802.11a and 802.11g have the same security problems as 802.11b.

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 modulation 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 (Frequency Hopping Spread Spectrum). The HomeRF standard uses 128-bit Blowfish encryption. An IV (Initialization 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 authentication 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 cannot 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 communication in the 5.15 – 5.3 GHz and the 17.1 – 17.3 GHz spectrum. HIPERLAN types 1 and 2, HIPERACCESS 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 encryption 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 restricts 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 authentication, both the access point and the mobile terminal can authenticate each other.

IPSec

Many application-specific security mechanisms have been developed in a number of application areas, including electronic mail (S/MIME, PGP), client/server (Kerberos), Web access (Secure Socket Layer), and (Stallings, 1999). By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but for all security-ignorant applications.

IPSec ensures a security level high enough even for the most critical applications. IPSec offers added packet-level IP security but leaves the existing core. Internet infrastructure is untouched, as IPSec deployment requires no extensive changes in the Internet infrastructure. IPSec is an Internet Engineering Task Force (IETF) standard for protecting IP traffic and it can be used to protect any IP based service or application. The purpose of the IPSec protocol suite is to provide a standard, secure way for communicating by using the TCP/IP protocol.

IPSec is not a specific protocol for wireless environment. But to ensure an end-to-end security through the Internet, it seems to be the only available standardized way. A wireless node which tries to access the Internet communicates through an access point, which will translate the address of the Internet and the address of the node. IPSec and this address translation are however incompatible. Some solutions - not yet standardized – to this incompatibility problem exist. These solutions will be discussed below.

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services (Stallings, 1999). Two protocols are used to provide security:

- An authentication protocol based on the header of the protocol, *Authentication Header (AH)*
- A combined encryption/authentication protocol based on the format of the packet for that protocol, *Encapsulating Security Payload (ESP)*

Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address, in other words, a method by which IP addresses are mapped from one network to another to provide transparent routing to hosts (Network Address Translation (NAT) Tutorial, 2000).

An ISDN router as a NAT device with a public IP address is an example. The router is connected to hosts in an internal network space and through an ISP to Internet. From the point of view of these hosts the Internet connection is normal. From the Internet it seems that there is a private network with a single device as a gateway (the ISDN router doing NAT) and the internal topology of the private network is invisible (SSH NAT Traversal Toolkit, 2001).

The popularity and growth of the Internet has led to a shortage of valid IP addresses. Network Address Translation is a short-term solution for this IP shortage. The NAT solution provides a growth path toward the next IP version (IPv6) , which is a much longer-term solution. However, the future of NAT seems set, as it is likely to function as a translator between the old (IPv4) and new (IPv6) IP networks.

As the basis of building VPN solutions, IPSec can no doubt be regarded as the most powerful building block being standardized at the moment (Salonen, 2001). However, as it is in a sense a new technology adding new features to existing already standardized technology, problems in the integrating process may occur . The emergence of NAT has, however, led to some complications from a network security point of view. A serious incompatibility problem exists between NAT and IPSec, the de-facto packet level security solution for the Internet of today - and possibly also tomorrow. An acceptable solution to this problem is a prerequisite to the use of IPSec for network security solutions in WLANs in general and especially in WLANs with mobile network nodes.

Proposed solutions to the IPSec and NAT incompatibility problem are *IPSec Pass-through, Realm Specific IP (RISP)* and *NAT Traversal* (SSH NAT Traversal Toolkit, 2001). In *IPSec Pass-through* the NAT gateway is configured to pass all IPSec traffic through untouched. This solution works fine if there is only one host behind the NAT gateway. *RISP* basically removes the need for NAT an preserves the end-to-end nature of IPSec traffic by leasing public IP addresses to hosts behind the NAT gateway. The weakness of RISP that every host behind a NAT gateway requires changes. *NAT Traversal* is based on a modification in the IKE negotiation protocol of the IPSec stand. Further modifications in the network infrastructure ar not needed. The NAT Traversal solution to the IPSec and NAT incompatibility problem is supported by several Internet-Drafts published by the IETF Internet Security Protocol (ipsec) Working Group (Adoba, 2001) (Huttunen, Dixon, Swander, Sierwald, Stenberg, Kivinen, Volpe and DiBurro, 2000) (Huttunen, Dixon, Swander, Kivinen, Stenberg, Volpe and DiBurro, 2001).

Bluetooth

The Bluetooth technology relies on frequency hopping and time multiplexing. The 2.4 GHz ISM band is used and the aggregated data rate is 1 Mbps. Bluetooth supports both point-to-multipoint data communication and point-to-point voice communication. The standard supports up to eight devices per piconet. The range is up to 10 m.

The technology was designed to connect mobile devices over a personal and private connection. Three security levels are defined (SIG Security, 2001):

- Level 1: No authentication is needed
- Level 2: Authentication depends on the type of service
- Level 3: Authentication is always needed

The technology supports application/link-layer authorization, authentication and encryption (Vainio, 2000) (Marks, 2000). Two trust levels are recommended, a Trusted Device Level with unrestricted access to services and an Untrusted Device Level with restricted access to services.

The Bluetooth device address is the 48-bit IEEE address. It is unique and public. Authentication involves a Personal Identification Number (PIN), the device address and a random number shared by the two communicating devices. They form a 128-bit initialization key which is used in a one or two way authentication. Once a trusted pairing is established, the codes can be stored within the device to allow more automatic/simple connections. A semi-permanent link key is generated and this key is also used for authentication.

After authentication, the link can be encrypted at various key lengths up to 128 bits (8 – 128 bits). The encryption scheme is flexible and allows devices to negotiate for the smallest common key length of the link. The architecture also supports authorization of different services to upper software stacks.

Wireless Network Example

A Wireless LAN – the MediaPoli Network - based on the Otaniemi Campus Network has been chosen to work as a testbed in Arcada Polytechnic. The network was designed by the company Otaverkko Oy (Otaverkko Oy - expert in telecommunications of the future, 2001) and by the HUT (Helsinki University of Technology) research community. Otaverkko Oy is a company established to set up, administer, maintain and develop the Mediapoli development environment. Arcada Polytechnic is a shareholder of the company Otaverkko Oy.

MediaPoli is based on a high capacity fixed network and a wireless broadband network. The wireless network consists of around 70 Wireless MediaPoli access points planted around the Otaniemi Campus and near-by companies. Figure 6 illustrates the coverage of the Wireless MediaPoli Network. The coverage areas are located in the following way: Arcada and Spektri Business Park (node 1), HUT (2-

6),Technical Research Centre of Finland (7), Center for Scientific Computing (8), Science Park Innopoli (9), Otaniemi Shopping mall (10) and the Student Union of HUT (11). Links to these organizations can be find in (MediaPoli - unique testbed for new innovations, 2001).

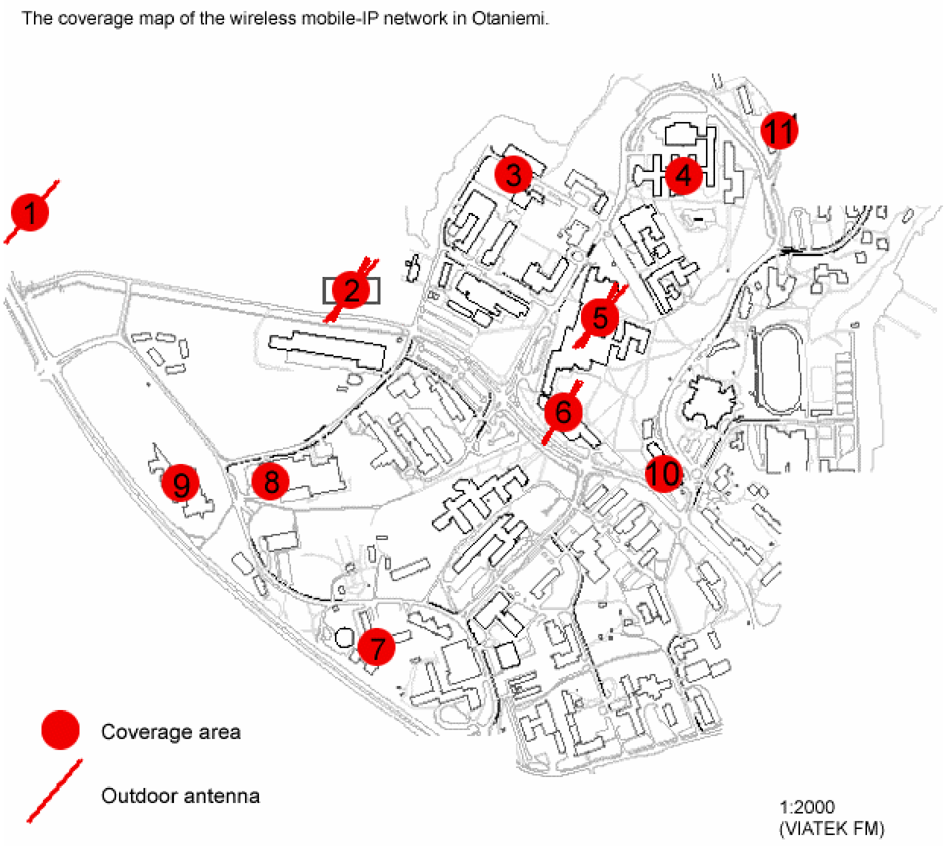
The coverage map of the wireless mobile-IP network in Otaniemi.
1
2
3
4
5
6
7
8
9
10
11
Coverage area
Outdoor antenna
1:2000
(VIATEK FM)

Figure 6. The coverage map of the Wireless MediaPoli Network in Otaniemi Campus.

The WLAN is based on the IEEE 802.11b protocol. The technology enables 1 - 11 Mbps Internet access via the wired, high speed MediaPoli backbone. The network is accessed using either DHCP (ISC Dynamic Host Configuration Protocol, 2001) or extended Mobile IP (MediaPoli - unique testbed for new innovations, 2001). The extended Mobile IP, developed at HUT, provides access and support for fast roaming.

MediaPoli is a unique testbed for new innovations, products and services. This development environment is based on a high-capacity fixed and wireless broadband network. This includes high performance IP routers, optical fiber based cabling, ATM technology and Gigabit-Ethernet technology.

A main objective is to provide an excellent platform for enterprises and research institutes to develop and evaluate new technologies, ideas and products. The network also provides an opportunity for operators, service and content providers, and content packagers to develop and evaluate business models of the future information society. Evaluation of end user behavior and user benefits from new services is another important issue.

Many examples of projects using MediaPoli are available at (MediaPoli - unique testbed for new innovations, 2001). Key research areas are:

- security, data confidentiality, authentication, electronic payment
- content provision, wireless multimedia, multimedia broadcast
- information processing, information search
- user interfaces and usability
- client/server and client/server technologies

- push technology
- proxies and intelligent agents
- mobility, mobile computing, mobile-aware applications, location aware applications
- communication protocols
- transmission media

Services offered in MediaPoli include

- *connection services* like broadband LAN, wireless LAN, HTTP proxy, and e-mail
- *multimedia services* like media servers, live streaming, video-on-demand, and multipoint video conferencing
- *data communication services* like, e-mail lists, database services, learning environment, and web hosting

Wireless MediaPoli operations started in 1998. Security features were handled by WEP and SSH. Today, SecGo Solutions´ VPN information security solutions are deployed. The SecGo Crypto IP VPN solution was chosen because it enables the use of various methods for user authentication. Users can be authenticcated reliably with , for example, smart cards or USB token. SecGo Crypto IP is a strong encryption and PKI based VPN solution. The software also enables secure remote VPN connections over NAT (Network Address Translation) (SecGo Solutions and Otaverkko to co-operate, 2001) (VPN for Service Providers, 2001).

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

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

Adoba, B. (2001). IPsec-NAT Compatibility Requirements, 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-nat-reqts-00.txt

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

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

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

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

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

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

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.htm

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

Huttunen, A., Dixon, W., Swander, B., Kivinen, T., Stenberg, M., Volpe, V., & DiBurro, L. (2001). UDP Encapsulation of IP-sec Packets, 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-01.txt

IP Security Protocol (ipsec). (2002). Internet Engineering Task Force (IETF). Working Group. Retrieved March 14, 2002 from the World Wide Web http://www.ietf.org/html.charters/ipsec-charter.html

ISC Dynamic Host Configuration Protocol (DHCP). (2001). Internet Software Consortium. Retrieved November 10, 2001 from the World Wide Web http://www.isc.org/products/DHCP/

Johnsson, M. (2000). HiperLAN2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band. White Paper. Retrieved September 21, 2001 from the World Wide Web http://www.hiperlan2.com/presdocs/site/whitepaper.pdf

Kesarev, K. (1997). Security level and solutions in wireless and mobile data transfer. Seminar report. Retrieved November 20, 2001 from the World Wide Web http:/www.tml.hut.fi/Opinnot/Tik-110.300/Tehtavat/mobile_wireless/security_2.html

Knight, W. (2000). 3G: Will 3G devices be secure? ZDNet UK, 23rd August. Retrieved November 20, 2001 from the World Wide Web http://news.zdnet.co.uk/story/0,,s2080988,00.html

Marks, L. V. (2000). What's what in wireless ?. IBM developer Works. Retrieved October 9, 2001 from the World Wide Web http://www-106.ibm.com/developerworks/library/wi-what/?dwzone=wireless

MediaPoli - unique testbed for new innovations. (2001). Retrieved November 29, 2001from the World Wide Web http://www.mediapoli.com/

Muller, M. J. (2001). Bluetooth Demystified. USA: McGraw-Hill.

Network Address Translation (NAT) Tutorial. (2000). International Technology Publishing. Retrieved November 11, 2001 from the World Wide Web http://www.itp-journals.com/Network_address_translation_NAT_page1.htm

Otaverkko Oy - expert in telecommunications of the future. (2001). Retrieved November 29, 2001 from the World Wide Web http://www.otaverkko.fi/inenglish.htm

Price, W., & Elkins, M. (2000). Extensions to TLS for OpenPGP keys, 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-openpgp-01.txt

Rysavy, P. (1998). Planning and Implementing Wireless LANS. Network Design Manual. Retrieved November 1, 2001 from the World Wide Web http://www.networkcomputing.com/netdesign/wlan3.html

Saarinen, Markku-Juhani. (1999). Attacks Against The WAP WTLS Protocol, University of Jyväskylä, Jyväskylä, Finland. Retrieved November 20, 2001from the World Wide Web http://www.jyu.fi/~mjos/wtls.pdf

Salonen, M., Virtual Private Networks: IPSec operability with NAT, *SecGo News on Network Security* 1/2001, Finland.

Schneier, B. (1996). *Applied Cryptography Protocols, Algorithms and Source Code in C. Second Edition*. USA: John Wiley & Sons.

SecGo Solutions and Otaverkko to co-operate. (2001). Press release. Retrieved November 10, 2001 from the World Wide Web http://www.secgo.com/6i.htm

Securing WAP Environments. (2000). White Paper. Retrieved June 17, 2001from the World Wide Web http://www.Europe.F-secure.com/products/white-papers/sec_wap_env.pdf

SIG Security. (2001). *Säkerhet vid trådlös datakommunikation* (in Swedish). Sweden: Studentlitteratur.

SSH NAT Traversal Toolkit. (2001). White Paper. SSH Communications Security. Retrieved November 27, 2001 from the World Wide Web http://www.ssh.com/tech/whitepapers/SSH_NAT_Traversal_Toolkit.pdf

Stallings, W. (1999). *Cryptography and Network Security. Principles and Practice*. Second Edition. USA: Prentice Hall.

Stallings, W. (2000). *Network Security Essentials. Applications and Standards.* USA: Prentice-Hall.

Steele, R., Lee, C.-C., & Gold, P. (2001). *GSM, cdmaOne and 3G Systems*. USA: Wiley & Sons.

Transport Layer Security (tls). (2002). Internet Engineering Task Force (IETF). Working Group. Retrieved March 14, 2002 from the World Wide Web http://www.ietf.org/html.charters/tls-charter.html

WAP Forum Releases. (2002). Retrieved March 10, 2002 from the World Wide Web http://www.wapforum.org/what/technical.htm

Vainio, J. T. (2000). Bluetooth Security. Retrieved October 9, 2001 from the World Wide Web http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

VPN for Service Providers. (2001). White Paper. SecGo Solutions. Retrieved November 10, 2001 from the World Wide Web http://www.secgo.com/docs/secgo_sp_wp_010814.pdf

What is RS4?. (2000). Crypto FAQ 3.6.3. RSA Security. Retrieved June 17, 2001 from the World Wide Web http://www.rsasecurity.com/rsalabs/faq/3-6-3.html

Wireless LAN Security. (2001). White Paper. Retrieved June 16, 2001 from the World Wide Web http://www.wlana.com/learn/security.htm

Biographies

Kaj J. Grahn, Dr. Tech., is presently senior lecturer in Telecommunications at the Department of IT and Electronics of Arcada Polytechnic, Espoo, Finland. He is also Program Manager of the Electrical Engineering Programme.

Göran Pulkkis, Dr. Tech., is presently senior lecturer in Computer Science and Engineering at the Department of IT and Electronics at Arcada Polytechnic, Espoo, Finland.

Jean-Sebastien Guillard is a student at ENSEIRB - Ecole Nationale Superiéure d’Electronique, Informatique et Radiocommunications, Bordeaux, France . A part of his final thesis work on Wireless Networks was done at Arcada Polytechnic, Espoo, Finland in summer 2001. Currently he is working for Accenture in Paris, France.