
Security Aspects of Mobile Communication Systems

Jan Pelzl and Thomas Wollinger

Horst Görtz Institute (HGI) for Security in Information Technology,
Ruhr University of Bochum, Germany
{pelzl,wollinger}@crypto.rub.de

1 Introduction

In recent years, applications have increasingly moved from wired to wireless. Former localized applications (e.g. desktop computers, phones) are now wireless and, therefore, movable. The convenience and acceptance of wireless and agile products yield an increasing demand for similar products in cars. Additionally, car manufacturers can reduce manufacturing costs by substitution of wired applications. The massive amount of cables in cars adds to cost and weight and can be avoided with wireless applications. Hence, we will see not only wireless entertainment applications, but also car functions move to wireless connections.

Communication of data using the air as a channel is very vulnerable to attacks. The reason that the attacker can easily tap the channel using radio receivers. The attacker is able to read, change, or delete messages. This can be a tremendous problem, leading to great financial losses for manufacturer even if the attack targets less important features in cars. The loss of confidence in car brands due to malfunctions in electronic devices is a concern of today's manufacturers. An attacker could invoke malfunctions of simple services such as power windows or air conditioning. The driver will probably return the car and never buy the same brand again.

Nowadays, several protocols for wireless communication can be found to be used for any new application that might be integrated in future cars. These include applications for in-car communication, car-to-car communication, and far field communication. However, we have to analyze these systems carefully in order to understand their security limitations. In this chapter, we introduce the most important standards for wireless communication and show associated security implications. All wireless systems can be structured by the designated application focus:

- *Far field communication:* Cell phone networks such as the Global System for Mobile Communication (GSM) and the Universal Mobile Telecommu-

nication System (UMTS). These systems can be used for several services such as traffic information, toll billing, weather information, local information services, and dynamic routing.

- *Car-to-car and hot-spot communication:* Wireless network standards wireless LAN (WLAN) and HiperLan/2 are appropriate for small-range data interchange between cars. Applications are, e.g., safety systems, ad-hoc networking between cars, remote diagnosis, and hot-spot communication (e.g., at gas stations).
- *In-car communication:* Possible applications of Bluetooth, ZigBee, DECT, and IrDA include data exchange from sensors to the control network of the car, PDA data interchange with car networks, and identification with keys.

For each standard we first give a short description of the architecture focusing on the part providing the security services. In addition, we list the security services as well as the security shortcomings of the standards.

Finally, a brief comparison of all standards regarding technical and security related aspects is given in Table 1.

2 Global System for Mobile Communication (GSM)

In the 1980s, most mobile cellular systems were based on analog technology. The Global System for Mobile communication can be considered as the first digital system. In 1982, the idea for an European standard for mobile communication over the band 900 MHz was born. By 1985 Germany, France, and Italy had signed an agreement for development of such a system. In 1991 the first GSM system was established in Genf. Today, GSM is a digit mobile telephone system that is widely used in Europe and other parts of the world.

In the car environment GSM can be used for far-field communication. Examples of an application could be remote diagnosis or on-board Internet. GSM can be used for transmitting the necessary data wirelessly to the manufacturer who analyzes the diagnosis data or for the exchange of data with the Internet provider. For the first application it is of great importance that the data arrives correctly to allow a complete diagnosis, whereas for the second application we want mainly to have a reliable system to guarantee consumer satisfaction. An example for current use of GSM in the automotive is “Toll Collect”, a toll collecting system for German highways. However, security plays a central role in keeping the transmitted information private.

2.1 Overview

In this subsection we describe very briefly the main parts of the GSM network, concentrating on the part applying the security mechanisms.

Mobile Station (MS): The mobile station consists of the hardware (the cell phone) itself and the Subscriber Identity Module (SIM). The phone is

uniquely characterized through the International Mobile Equipment Identity (IMEI) and provides the encryption algorithm A5. The A5 algorithm achieves encryption for the data transmission. The SIM is a smart card providing the user with access to the subscriber services. A four-digit PIN (Personal Identification Number) identifies the user to the chip card. In addition, the following information is stored on the card: IMSI (International Mobile Subscriber Identity), the user-specific symmetric Key K_i (128 bit), the A3 algorithm for challenge-and-response authentication and the A8 algorithms to generate the session key.

Base Station Subsystem (BSS): The BSS handles the connection between MS and the Network and Switching Subsystem (NSS). The BSS can be divided into two parts: (a) the Base Transceiver Station (BTS) and (b) the Base Station Controller (BSC).

Network and Switching Subsystem (NSS): The main aim of the NSS is to manage the communication between the different users, including the storage of information concerning the subscribers and the coordination of their mobility. NSS consists of the Mobile services Switching Center (MSC), the Gateway Mobile services Switching Center (GMSC), the Home Location Register (HLR), the Visitor Location Register (VLR), and the Authentication Center (AuC) Equipment Identity Register (EIR).

HLR, VLR, and AuC are the components of the NSS important for security. HLR stores subscriber-related data, hence, also the cryptographically related data, like user keys. The VLR is a temporary database for visitors needed to ensure services. The network provider needs to deposit the encryption data and authentication of the MS. AuC verifies the identity of the user by providing authentication and encryption parameters.

Operation and Support Subsystem (OSS): The OSS is connected to the NSS and to the BSC and allows for monitoring and controlling the system.

2.2 Security of the GSM network

In this section, we will provide the reader with an overview of the security aspects implemented in GSM. GSM provides two cryptographic protocols, namely to ensure authentication of the user to the network and to encrypt the data.

Authentication of the User to the Network: Authentication allows the network provider to uniquely identify the user by checking if the user (or better the chip card of the user) knows the IMSI and the user key K_i . Authentication avoids therefore the placing of calls another person's account. Fig. 1 illustrates the authentication between user and network. In the first step the user sends the TIMSI (Temporary IMSI) to the base station. The idea behind the TIMSI is to hide the identity of the MS by frequently updating this number during each location update procedure. The TIMSI allows the network to get the user's key K_i from the database. In the second step, the network challenges the SIM card with a 128-bit random number. At this point

the two parties (SIM and network) are able to calculate the Signed Response (SRES) using the A3 algorithm. The cell phone is authenticated if the two results are equal.

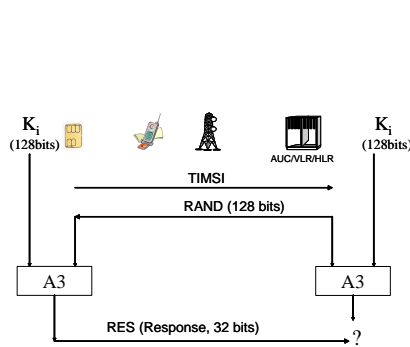


Fig. 1. GSM user authentication

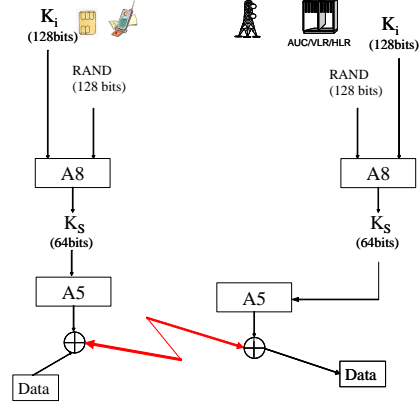


Fig. 2. GSM voice encryption

Voice Encryption: Data is transferred by air and, thus, can be easily eavesdropped by an attacker using radio receivers. Encryption is done using a session key K_S which is generated using the A8 algorithm (see Fig. 2). The input values to A8 is a random number RAND and the user key K_i . Note that K_S is valid at most for one communication. The cipher A5 uses K_S as input and produces the key stream to be XORed with the data.

2.3 Security Analysis

In this subsection we analyze the security features of GSM. It is important to understand the strengths but also the drawbacks of GSM. Using this knowledge an application designer is able to judge whether the system is sufficient in terms of security for the given application. For more detailed information the reader is referred to [13, 17].

Access control: Access control between the user and the SIM card is given by a secret PIN and, thus, does not allow (easy) unauthorized access. Note that the PIN is not a sufficient protection against serious attacks.

Temporary identity: The TIMSI will be newly assigned to the user at each location. Hence, it is very hard for an attacker to obtain a profile of the user.

Authentication: Authentication protects from unauthorized service access and ensures that the user pays only his/her phone costs. However, the

GSM network provides only authentication of the user to the network. The protocol does not identify the network to the user. Hence, false base station attacks are possible.

The second problem with authentication is based on the fact that the A3 and A8 algorithms are not specified in the GSM standard. Thus, the security of these algorithms relies on security-by-obscurity and therefore is not considered secure in general. The GSM standard committee recommended the use of COMP 128 for A3 and A8 which was broken in [4]. For this attack we need to perform 8 to 12 hours of calculations on the card to determine the user key K_i .

Key Establishment/Encryption Algorithm: Encryption protects user data; however, we need a stronger algorithm since the algorithm is broken and the key length is too short. In addition, encryption is only applied at the wireless interface (further security services are operator dependent). Thus, all information including TIMSI, RAND, SRES, K_s as well as the communication and signaling information are transmitted in clear within and between networks.

Transparency: Security features operate without user assistance. Thus, there is no indication to the user that encryption is activated. No explicit confirmation of properly accomplished authentication and correct authentication parameters are given when subscribers roam etc.

Channel Hijack: Protection against radio channel hijack relies only on the encryption mechanisms. However, encryption is not strong enough or is not used at all in some networks.

Inflexibility: The security functionality is inadequate and not flexible to upgrade over time. There will always be security holes in practical applications and, therefore, it is important to have mechanisms to upgrade cryptographic primitives or flawed software.

3 Universal Mobile Telecommunication System (UMTS)

The Universal Mobile Telecommunication System is envisioned as the successor to GSM. Hence, UMTS will be used in far-field communication, providing applications like DynRouting, Remote Diagnosis and Internet in the car. The main difference from GSM is that UMTS handles a higher data rate (up to 2 Mbps) per mobile user and that most security limitations of GSM are no longer present.

3.1 Overview

The UMTS standard is an extension of existing networks introducing the new components UTRAN, RNC, and Node B. In the following describe the functionality of the new components in more detail. All the other existing components such as the HLR can be extended for UMTS. The handsets must

be developed from GSM. The UMTS User Equipment (UE) is separated from the Mobile Equipment (ME) and the UMTS Subscriber Identity Module card (USIM), as in the GSM network.

UTRN and RNC: UTRAN is subdivided into individual Radio Network Systems (RNSs). The RNC provides control for each RNS. One or more Node B elements are connected to the RNC. RNC provides central control for the RNS elements, and handles protocol exchanges, central operation, and maintenance.

Node B: The Node B provides the radio transmission and reception. The main task of the Node B is to connect the UE (via radio interface) and the RNC (via asynchronous transfer mode). In addition, the Node B takes part in the power control of the UE.

3.2 Security Analysis

The security of UMTS is built on the security of GSM. The designers adopted the security features from GSM that have been proven to be needed and robust. On the other hand UMTS tries to ensure compatibility with GSM in order to ease inter-working and hand-over. Furthermore, UMTS corrects problems with GSM and adds new security features necessary to secure new services, e.g. authentication of the network. In the following we give a brief description of the main security features of UMTS.

UMTS Authentication and Key Agreement (UMTS AKA): Authentication and key agreement in UMTS is similar to the one used in GSM [2]. The challenge-and-response protocol used in UMTS is enhanced to be able to provide mutual authentication. Fig. 3 illustrates the performed protocol. After the VLR (SGSN) requested the authentication vector (AV), the AuC responds with the generated quintets ($RAND$, $XRES$, CK , IK , $AUTH$). The $AUTH$ contains a sequence number (SEQ), a message authentication code (MAC) and an authentication management field (AMF).

In a second step the network can challenge the user, by sending a random number ($RAND$) and the $AUTH$ to the USIM. The user has the possibility to verify the received challenge data. This data could only have been constructed by someone possessing the secret key K_i . The USIM can also verify the freshness of the data by checking the SEQ . If all the tests are successful the network has authenticated itself to the user. The USIM can then generate the confidentiality key (CK), the integrity key (IK), and the response (RES). At the end the user sends the RES to the network and if $XRES$ equals RES , the two parties can start to communicate securely.

Confidentiality and integrity protection: In UMTS the security terminates in the RNC, which is the reason for the RNC being located closer to the core network than the Node-B (base-station). Using the established keys (IK and CK) one can start the confidentiality and integrity protection services. The confidentiality protection applies to both user data and the as-

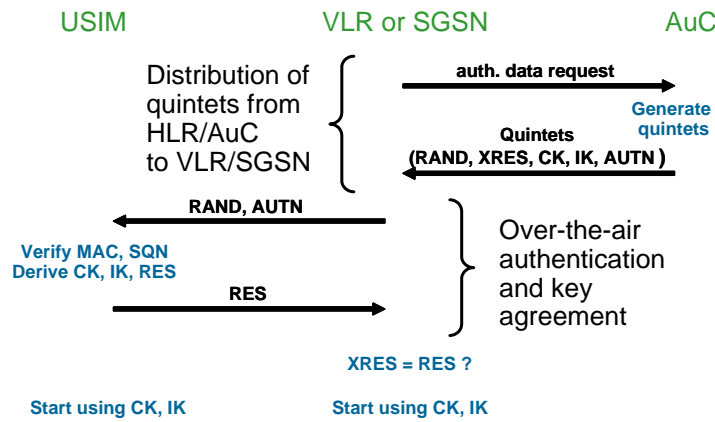


Fig. 3. UMTS message flow [18]

sociated system signalling data using the $f8$ algorithm, realized by KASUMI algorithm [3].

The algorithm to provide integrity is called $f9$ and is also realized with the KASUMI algorithm. Note that the UMTS restricts integrity protection to the system signalling. Thus, the user data is not integrity protected. Another limitation of the integrity protocol in UMTS is that only a 32-bit long integrity check value is used.

Security in the UMTS core network: Network Domain Security (NDS) is needed to secure all important control plane protocols in the core network. There exists already a protection suite for the IP-based protocols, namely IPsec. Hence, this was the natural choice for security protection and furthermore it is implemented in the network layer and, thus, no changes are required to the target protocols [1].

4 Wireless LAN

Wireless Local Area Networks (WLANs) are based on a standard defined by the Institute of Electrical and Electronics Engineering in 1997 (IEEE 802.11) [11]. WLANs offer the possibility to easily set up networks and extend cable-based networks. Easy maintenance, flexibility and small devices make WLANs in particular interesting for embedded applications. Furthermore, WLANs have emerged in temporary networks (exhibitions, ad-hoc networks) or airports and downtown areas (hot spots).

Most current WLAN products are based on the standard IEEE 802.11b from 1999. The so called Wi-Fi Alliance certifies interoperability of Wireless Local Area Network products based on the IEEE 802.11 specification. Currently the Wi-Fi Alliance has over 200 member companies from around the world, and over 1250 products have received Wi-Fi [19].

Since 2001, major security problems of the standard are known and, finally, in 2004 a new standard addressing all security limitations was published (IEEE 802.11i). Unfortunately, most circulating products are not able to upgrade to the new standard.

The following two sections provide a brief overview of the standard with emphasis on security aspects. For detailed technical information and on WLAN security, the interested reader is referred to [6] and [11].

4.1 Overview

Radio Technology:

Wireless LAN systems approved in Europe use the ISM (Industrial-/Scientific-/Medical-) band between 2.4 and 2.48 GHz. It can be used free of charge and without any extra approval. The maximum transmission power is restricted to 100 mW. IEEE 802.11 specifies data transmission via Spread Spectrum with Frequency Hopping (FHSS) or Direct Sequence (DSSS). In the German 2.4 GHz band, 13 frequency channels with a bandwidth of 5 MHz are available. Three channels can be used simultaneously without interference (see Fig. 4).

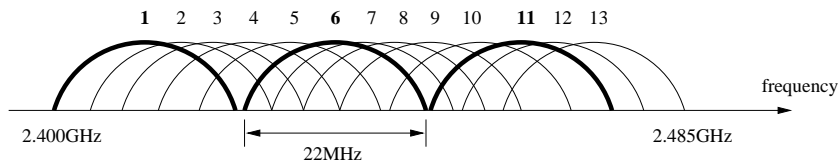


Fig. 4. WLAN channels

A single radio cell has a range between 10 and 150 m, depending on the environment, e.g., allowing for in-car and car-to-car communication at high data rates. Future radio systems (802.11n) will use the 5 GHz band with 19 approved channels (no overlap) in total.

Maximum throughput is 11 Mbit/s (802.11b) and 54 Mbit/s (IEEE 802.11g). Note that IEEE 802.11 does not guarantee a certain bandwidth since the maximum throughput depends on the number of clients and the quality of the radio link.

Network Architecture

IEEE 802.11 specifies two different architectures for wireless LANs: ad-hoc mode (IBSS=Independent Basic Service Set) and infrastructure mode (BSS=Basic Service Set). In ad-hoc mode, two or more (mobile) clients communicate directly over a radio link, whereas in the latter mode all communication is centralized via an Access Point (AP).

The infrastructure mode allows for roaming: An overlapping radio network with many access points can be constructed. The connection to a client can be retained while the client moves from one radio cell to another.

IEEE 802.11 entitles the union of many BSS as an Extended Service Set (ESS), with the connection network as Distribution System (DS). When a client enters the range of one or more APs, the APs broadcast a signal including a Service Set Identifier (SSID). The best AP in terms of signal strength is selected and the client turns to the AP channel. A client periodically surveys all channels in order to check for stronger or more reliable APs.

4.2 Security Analysis

Old standard IEEE 802.11

Security mechanisms are defined in IEEE 802.11 and, recently, in IEEE 802.11i. IEEE 802.11a, b, g and h do not describe additional security mechanisms. In the following, all mechanisms of the original standard IEEE 802.11 are outlined. Note that all mechanisms are fundamentally flawed and do not provide reliable security for sensitive information.

- (E)SSID: The (Extended) Service Set Identity provides network names and is always sent in clear and thus, can be eavesdropped. Users can allow for any (E)SSIDs or only for certain (E)SSIDs. Access points usually broadcast (E)SSID unless configured otherwise, which is not always possible. Even if disabled, SSIDs can still be obtained from (secondary) control information sent by APs.
- Media Access Control (MAC) Address: Though not specified in the standard, APs can grant access for only certain MAC addresses. In this case all access lists have to be edited by hand. Furthermore, MACs can easily be manipulated in wireless environments such that solely MAC filtering is no security enhancement.
- Wireless Equivalent Protocol (WEP): The goal of WEP was to provide equivalent security as in cable networks, including
 - Integrity: For each data packet, a 32-bit checksum (CRC32) is computed and attached to the data (ICV=Integrity Check Vector), as shown in Fig. 5. With encryption enabled, the data packet with ICV is encrypted. After decryption, the receiver checks the ICV. CRC32 can detect (transmission) errors with high probability. Cleverly swapped

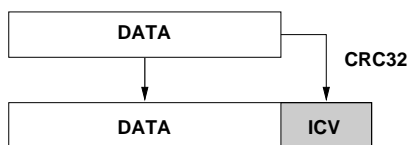


Fig. 5. WEP integrity check

data bits cannot be detected since due to the linearity of CRC and the simple XOR encryption, the CRC can also be manipulated.

- Authentication: Two authentication modes are possible in connection with WEP encryption: “Open” with no authentication and “Shared Key”. The latter mode accomplishes a challenge response protocol. The AP generates 128 pseudo random bits and sends them to a client (challenge). The client encrypts the challenge and sends the encrypted bits back to the AP (response). The client has authenticated properly if the AP can decrypt the response. Note that the authentication is unilateral, i.e., the AP does not authenticate itself to the client.

This authentication protocol is completely flawed: An attacker can record an authentication step, and build the XOR of challenge and response. The resulting bits are the first bits of the key stream; thus, the attacker can authenticate himself from now on. Furthermore, messages can be faked with the help of computed key stream bits.

- Confidentiality: The key together with an initialization vector (IV) generates a pseudo random bit stream (stream cipher RC4) and XORs the bit stream with the data bit stream. Encryption and decryption are similar operations. The IV changes with every packet to ensure non-deterministic encryption. After encryption, the IV is appended in clear to the cipher text (see Fig. 6).

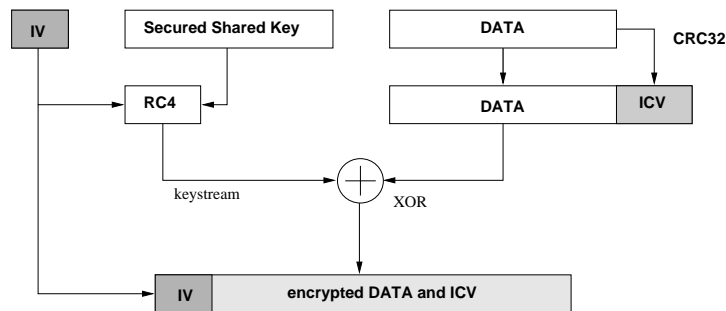


Fig. 6. WEP encryption

The IV is far too short since 24 bit yield only approximately 16.8 million different IVs; thus, if created at random, repetitions will occur every 4000's IV on average.

Two key lengths, 40 bit and 104 bit, are specified. Four 40-bit keys or one 104-bit key can be used. The same key is used for the whole network, and thus has to be provided to every client and AP. No key management is specified in IEEE 802.11. Keys are manually distributed and statically configured, implying infrequent changes. Thus, large volumes of traffic are encrypted with the same key, which lets cryptanalysts crack the key in a few days. Even the use of 40-bit keys with frequent changes is not advisable since conventional PCs can decrypt messages with "brute force" in a few days.

Additionally, RC4 suffers from some weaknesses which can be exploited by statistical tests [15]. The Internet offers many tools for automated attacks on WEP. Taking all aspects into account, WEP offers very little security.

New Security Standard IEEE 802.11i

The new security standard removes most security limitations of WEP. Before the approval of IEEE 802.11i in June 2004, the so-called Wireless Protected Access (WPA) was introduced as a stopgap method before the full standard. Many parts of the i-standard have already been introduced. The enhanced security standard allows for the following features:

- Mutual authentication: Client and AP authenticate each other.
- Temporary Key Integrity Protocol (TKIP): Each station gets a separate key for confidentiality, which is changed frequently.
- Extensible Authentication Protocol (EAP): Authentication involves a device proving its identity to another device. EAP enables authentication with an authentication server. The possibility of PKI-based authentication is given.

General Security Limitations of WLAN

- Uncontrolled propagation of radio waves: though specified, the range of WLAN can exceed 150 m depending on the quality of transmitter and receiver. Thus, eavesdropping is possible even beyond the range stated in the standard.
- WLAN (as well as any other radio-based system) can be jammed, regardless of any security service present.
- Profiling: Sending MAC addresses always in clear does allow for generation of profiles of mobile users.

5 Bluetooth

Bluetooth is an open standard (IEEE 802.15.1) for close-up range wireless voice and data communication [11]. The development of Bluetooth originated from the Bluetooth Special Interest Group in 1998 with currently more than 2500 manufacturers [5]. The specification is in version 1.1 at present; version 1.2 is close to approval.

5.1 Overview

Like WLAN, Bluetooth works with 79 channels in the ISM band (2400-2480 MHz). The data is modulated with Gaussian Frequency Shift Keying (GFSK) and transmitted in Time Division Duplex (TDD) in combination with Frequency Hopping Spread Spectrum (FHSS). A time slot is 625 s and the frequency changes 1600 times per second. The asynchronous connection less (ACL) transmission reaches a maximum throughput of 723.2 kbit/s in one direction and 57.6 kbit/s in the other (asymmetric) or 433.9 kbit/s in both directions (symmetric). Voice transmission is accomplished with up to 3 synchronous connection oriented (SCO) channels 64 kbit/s each. Voice is encoded with Pulse Code Modulation (PCM) or Continuous Variable Slope Delta (CVSD) modulation.

The range of Bluetooth devices is 10-100 m depending on the transmission power (1-100 mW). To save power consumption, energy-efficient modes (sniff-, park-, and hold-mode) are specified. An adjustment of the transmission power is possible [6].

To guarantee the interoperability of all Bluetooth devices, different application profiles have been established: Generic Access Profile, Serial Port Profile, Generic Object Exchange Profile, Headset Profile, LAN Access Profile, Personal Area Networking (PAN) Profile, and more.

For identification, each device has a (worldwide) unique 48-bit hardware address (Bluetooth Device Address).

5.2 Security Analysis

Bluetooth specifies integrity protection and cryptographic mechanisms to ensure confidentiality and authentication. All mechanisms are implemented in hardware and, thus, are available at the data link layer. The cryptographic protocols are based on *link keys* negotiated during the *pairing*.

If two devices want to establish a secure communication, they have to be *paired*. Thus, a 128-bit *combination key* depending on both device addresses and random numbers is generated. For secure transmission of both random numbers, a 1- to 6-byte PIN has to be entered into both devices. If one PIN is fixed (as preset of the device) it has to be entered into the other device. Two devices with the same fixed PIN cannot be paired.

The standard allows for two other possibilities to generate session keys besides the use of the combination key:

- *Unit keys* are generated before the first use of a device (and cannot be changed). They are used if the memory of a device is constrained and too small for saving more keys or if a device has to be accessible to a huge group of devices.
- *Master keys* can be negotiated temporarily between devices if a master wants to use the same key with many devices. Master keys are only used in multi-point connections and are always sent to the clients encrypted with the session key.

Security Services

- Integrity protection: Integrity is protected with a CRC. As in the WLAN case, malicious manipulations cannot be detected if the CRC is also manipulated (see Section 4).
- Authentication: Authentication is based on challenge response protocol using a symmetric cipher. Mutual authentication is achieved by two-sided unilateral authentication. The verifier sends a random number to the claimant, who generates a 32-bit response of the number together with the session key and his device number. From the same input data, the claimant generates another 96-bit *authenticated cipher offset*. This (secret) offset can be used as input for the generation of further encryption keys. The verifier simply generates the same 32-bit string and verifies the response.
- Confidentiality: Encryption is *always* optional and can be established if at least one party is authenticated. The encryption algorithm E0 is a stream cipher. For each data packet, a new initialization vector is used (non-deterministic). Encryption is only applied during radio transmission. Before broadcast and after reception the packets are not encrypted (no end-to-end encryption).

Further Security Limitations of Bluetooth

- Authentication is done by the devices, not by the user itself.
- Bluetooth Device Addresses can be manipulated (flash memory).
- Possible eavesdropping and recording of (unencrypted) voice transmission (headset).
- Bluetooth can be jammed.
- Default settings are often insecure (PIN consists of zeros ...).
- The standard does *not* specify generation of random numbers.
- Man-in-the-middle attacks are possible even with authentication. Since encryption is implemented with a stream cipher, intercepted data can be manipulated if plain text (e.g., network address) is known.
- Interception of radio signals originating from Bluetooth devices (e.g. with Bluetooth protocol analyzer ...).

- Unique device addresses simplify generation of profiles. Device addresses are not only used during the setup phase, but also attached to most data packets.
- Achieved security does not exceed 84 bit, though a 128-bit key can be used [16].

For a detailed description of major Bluetooth weaknesses, refer to [12].

6 Further Wireless Standards

Besides the widespread standards GSM, UMTS, WLAN, and Bluetooth, there exists a variety of other interesting wireless solutions, with potential application to in-car and inter-car communication. The following sections provide a short overview of ZigBee, DECT, HiperLan/2, and IrDA.

6.1 ZigBee

The application focus of ZigBee is monitoring and control. Its goal is the provision of wireless communication for very small devices (e.g., sensors). Parts of ZigBee are standardized up to the network layer in IEEE 802.15.4. The application layer is defined in the ZigBee Alliance [21]. Therefore, ZigBee should not be used as a synonymous standard for IEEE 802.15.4.

ZigBee uses 16 channels in the 2.4 GHz band with a throughput of up to 250 kbit/s via Offset Quadrature Phased Shift Keying (O-QPSK). Additionally, one channel with 20 kbit/s is available at 868 MHz via Binary Phase Shift Keying (BPSK). Transmission is accomplished using the Direct Sequence Spread Spectrum (DSSS) together with the CSMA/CA protocol (see Section 4). ZigBee allows for similar modes of networking to Bluetooth. Additionally, ZigBee specifies self reorganizing networks. Major technical properties of ZigBee are low power consumption (≈ 0.5 mW) and medium range from 10-100 m. Good data integrity is achieved through high redundancy and dynamic channel selection.

The standard specifies a security toolbox for optional security functions such as authentication and encryption. The security services provides 32- to 128-bit AES. Key management is not specified.

6.2 DECT

Digital Enhanced Cordless Telecommunications (DECT) obeys the official ETSI standard for mobile communication networks for voice and data [8]. DECT is implemented in cordless telephones and can usually be found in offices, premises and private homes. DECT can also be used for bridging small distances (1-2 km) between provider and client. For interoperability between

different DECT devices, a General Access Profile (GAP) is specified. Interworking Profiles define interfaces to other networks such as ISDN. Mobile networks can be built from DECT devices. Different communication services can be found in so-called Application Profiles for specific applications. The DECT Packet Radio Service (DPRS) and DECT Multimedia Access Profile (DMAP) allow for connections with high throughput comparable to Bluetooth.

In Europe, DECT operates at 10 carriers in a reserved band from 1880-1900 MHz with Frequency Division Multiplex (FDM). Each carrier is time division multiplexed (TDMA) in 24 slots. Time Division Duplex (TDD) with 12 duplex channels per carrier yields 120 available duplex channels in total.

DECT supports different modes of operation:

- Single cell system: The whole DECT system consists of a fixed part and a portable part (e.g., cordless telephone and base station).
- Direct mode: Two DECT portable parts communicate directly with each other.
- Multi-cell system: DECT is multi-cell capable and supports roaming.

The standard provides security mechanisms against eavesdropping. Authentication is based on a challenge response procedure with a 128-bit long-term key which has to be entered into both devices at the beginning. A portable device has to authenticate itself against the fixed part. Mutual authentication (i.e., additional authentication of a fixed part against a portable part) is optional. Detailed information about the authentication specification can be found in [8]. The authentication algorithms A11 and A12 are not publicly available and the strength of the algorithms is not known.

The implementation of the key management has several degrees of freedom, i.e., it is possible to register a cordless phone at a base station without previous exchange of a long-term key.

Encryption of the transmitted data is optional and is realized with a stream cipher. The stream cipher is initialized with a 64-bit cipher key (CK) and an initialization vector (IV). In practice, encryption is almost always toggled off or not even implemented. If encryption is implemented, usually key sizes of 64 bit are used, which is considered as insufficient nowadays. As with the authentication algorithms, the encryption algorithm is not publicly known.

Unattached encryption, protocol analyzers allow for profiles of base stations (e.g. how often encrypted session are established etc.). Built-in baby phone functionality enables easy eavesdropping.

6.3 HiperLAN/2

High Performance Radio Local Area Network Type 2 (HiperLAN/2) is a standard of the European Telecommunications Standards Institute (ETSI) [9]. HiperLAN/2 is a competitor of IEEE 802.11. IEEE 802.11 can be seen as wireless Ethernet whereas HiperLAN/2 works like a wireless ATM. Media access is centralized, connection oriented and supports quality of service.

HiperLAN/2 uses the 5 GHz band from 5.15 to 5.35 GHz and 5.47 to 5.725 GHz with 19 different channels of 20 MHz each. Maximum throughput is 54 Mbit/s at a range of approximately 30 m indoor and 150 m outdoor. The transmission power is limited to 200 mW indoors and 1 W (EIRP) outdoors. Handover of mobile stations to different base stations is supported by HiperLAN/2 to supply large areas. Transmission uses Orthogonal Frequency Division Multiplex (OFDM) modulation and is time multiplexed (TDMA/TDD, Time Division Multiple Access, Time Division Duplex). Carrier access handling is centralized by the base station or a dedicated mobile station which assigns time slots of different lengths.

Establishing a communication with a mobile station requires the MAC address of the base station. Different cryptographic options are possible: encryption with a common derived key, mutual authentication, and encrypts with multi-cast keys provided by the base station. For each application, different keys are used. The session key for encryption is derived via Diffie-Hellman key agreement [7] and yields a DES or 3DES key. Weak and semi-weak keys are discarded. The base station initializes a new key exchange frequently. To keep keys fresh, multi-cast keys are assigned frequently by the base stations, and are encrypted with the session key. Encryption implements DES or 3DES in Output Feedback (OFB) mode.

The authentication keys are either pre-distributed symmetric keys (≥ 128 -bit) or asymmetric key pairs (RSA512, RSA768 or RSA1024). Key management with certificates and a Public Key Infrastructure (PKI) is possible. Authentication is realized with a challenge response protocol. The response is generated either with a MD5-HMAC or with an RSA signature according to PKCS#1 v1.5 [14]. Security risks arise with the possibility of a man-in-the-middle attack on stations, which have no direct connection (see [6]). Anyway, HiperLAN/2 is much more secure than IEEE 802.11 (see Section 4). Dynamic MAC addresses assigned by the base station avoids profiling.

6.4 IrDA

The Infrared Data Association (IrDA) is a non-profit organization and released the first specifications of a protocol for an infrared interface in 1994 [10]. This infrared interface was designed as a wireless alternative to the serial port. IrDA uses wavelengths in the range of 850-900 nm and defines data rates up to 16 Mbit/s. The average range is 0.2-2 m and depends on the transmission power. Data integrity is achieved with CRC16 (up to 1.152 Mbit/s) and CRC32 (above 1.152 Mbit/s). For a successful communication, both devices have to face each other. IrDA does not specify any cryptographic service; thus, no authentication and encryption is possible.

7 Conclusion

Wireless networks can have many advantages compared to cable-based solutions: they are easy to set up and easy to maintain, they can be implemented in devices of nearly any size and can have little power consumption. The variety of the presented solutions demonstrate a wide possible field of application. High-end wireless ATMs (HiperLAN/2) are just as feasible as ultra-low-power transmissions in the kbit range (ZigBee). Thus, nearly any cable-based network has its wireless counterpart. Table 1 gives a short summary of the technical properties and the security of all presented systems (see also [20]).

Table 1. Technical comparison of selected wireless standards and security features [20]

Market name Standard	GPRS/GSM 1xRTT/CDMA	UMTS 3GPP	Wi-Fi IEEE 802.11 a,b,g,h,i	Bluetooth IEEE 802.15.1	ZigBee IEEE 802.15.4
Application focus	Far field comm.	Far field comm.	Car-to-car comm.	In-car comm.	In-car comm.
System resources	16 MB+	16 MB+	1 MB+	250 kB+	4-32 kB
Battery life (days)	1-7	1-7	0.5-5	1-7	100-1000+
Network size	1	1	32	7-250	255/65,000
Bandwidth (kB/s)	56-128	56-14,000	800-54,000	720	20-250
Transmission range (m)	1,000+	1,000+	10-100	1-10+	1-100+
Success metrics	Reach, quality	Reach, quality, speed	Speed, flexibility	Cost, convenience	Reliability, power, cost
Security services: - Integrity - Authentication - Confidentiality	X unilateral (X)	X mutual X	X mutual (opt.) X (opt.)	X mutual (opt.) X (opt.)	X mutual (opt.) X (opt.)

Nevertheless, wireless protocols still have and will always have some serious penalties. Every wireless connection can be jammed, regardless of applied security services such as encryption. Thus, wireless devices should never be used for sensitive applications, e.g., applications which might harm or injure persons in cars in case of failure. Furthermore, the broad range of several wireless systems do not allow for clear localized restrictions of networks. Well-equipped attackers might always be able to eavesdrop any communication sent over the network. Strong cryptographic primitives and a diligent implementation of such algorithms and protocols can help to solve this disadvantage. Many common wireless systems still suffer from poorly designed security services (e.g., old IEEE 802.11, GSM). Using these systems demands security solutions beyond the (flawed) standards, e.g., virtual private networks (VPNs) or other end-to-end encryption mechanisms.

References

- [1] 3GPP. Network Domain Security; IP network layer security. 3G TS 33.210, 2004. <http://www.3gpp.org/>.
- [2] 3GPP. Security architecture. 3G TS 33.102, 2004. <http://www.3gpp.org/>.
- [3] 3GPP. Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: *f8* and *f9* Specification. 3G TS 35.201, 2004. <http://www.3gpp.org/>.
- [4] M. Briceno, I. Goldberg, and D. Wagner. GSM Cloning. 2003. <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>.
- [5] Bluetooth Membership Site. <http://www.bluetooth.org/>, 2004.
- [6] BSI - Bundesamt für Sicherheit in der Informationstechnik. Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte. Technical report, Projektgruppe “Local Wireless Communicatio”, 2003.
- [7] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.
- [8] European Telecommunication Standards Institute. ETSI EN 300 175-1, Digital Enhanced Cordless Telecommunications (DECT), Common Interface (CI) Part 1-8, 1992.
- [9] European Telecommunication Standards Institute. ETSI TR 101 683, HIPERLAN Type 2 Overview, 1992.
- [10] Infrared Data Association Site. <http://www.irda.org/>, 2004.
- [11] Institute of Electrical and Electronics Engineering. IEEE 802 LAN/ MAN Standards. <http://standards.ieee.org/getieee802>, 2004.
- [12] M. Jakobsson and S. Wetzel. Security weaknesses in bluetooth. In *Proceedings of the Cryptographer's Track at the RSA Conference (CT-RSA 2001)*, LNCS 2020. Springer, September 2001.
- [13] Wolfgang Rankl and Wolfgang Effing. *Handbuch der Chipkarten*. Hanser-Verlag, 1966.
- [14] RSA Laboratories, 1993.
- [15] A. Shamir, S. Fluhrer, I. Mantin. Weaknesses in the Key Scheduling Algorithm of RC4. In *Selected Areas in Cryptography - SAC 2001*, volume 2259 of *Lecture Notes in Computer Sciences*, pages 1-24. Springer-Verlag, 2001.
- [16] S. Lucks and S. Fluhrer. Analysis of the E_0 Encryption Scheme. In *Selected Areas in Cryptography - SAC 2001*, volume 2259 of *Lecture Notes in Computer Sciences*, pages 38-48. Springer-Verlag, 2001.
- [17] Klaus Vedder. Gsm: Security, services, and the sim. In Bart Preneel and Vincent Rijmen, editors, *State of the Art in Applied Cryptography*, volume 1528 of *LNCS*, pages 224–240. Springer-Verlag, 1997.
- [18] M. Walker. On the security of 3gpp networks. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 102–103. Springer, 2000.
- [19] WiFi Alliance. <http://www.wi-fi.com/>, 2004.
- [20] J.F. Wollert. Bluetooth, WLAN und ZigBee für die Automatisierungstechnik. *etz – Elektrotechnik und Automation*, 6:10–18, 2004. VDE Verlag.
- [21] ZigBee Alliance Site. <http://www.zigbee.org/>, 2004.