SECURITY *Special*

mobile telephones modern means of communication or source of uncalculated risks?

mobile telephon

modern means of communication or source of uncalculated risks?

The number of mobile telephones has increased steadily over the last few years. A proportion of one in eight persons in Germany today is telephoning per mobile phone. Of the over eight million telephones in use, roughly seven million are digital tele-phones belonging to the D1, D2 and E-plus networks. It is especially the number of digital mobile phones which is increasing so steadily.

Albeit, in addition to those benefits offered by mobile phones such as being able to be reached at all times and a variety of extras for telephoning, there are also dangers involved. These dangers have their origin in such devices, whether they have to do with the technology in and around the mobile unit or stem from intentional misuse.

- Mobile phones can cause disturbances by interfering with electrical and electronic equipment and systems.
Key concept: EMC (electro-magnetic compatibility).

- Mobile phones can be utilized for the unauthorized transmission of stored data.
Key concept: Industrial espionage.

- Mobile phones can be misused for purposes connected with bugging and the forwarding of confidential conversations.
Key concept: Confidentiality.

These dangers make the secured identification and siting of mobile phones in an operating mode necessary.

Interferences with electrical and electronic equipment

The danger here comes especially from digital telephones. Digital telephones transmit with a transmitting power of up to 2 Watts along with so-called “bursts” (occurrences where data clusters are conveyed in phases). This enables them to interfere with electrical and electronic equipment, meaning they can distort measurement readings, trigger control signals or interfere with the function on the whole. The danger risk is disproportionately smaller with analog C-Net telephones because they transmit steadily and do not have such pulsed signals. (No bursts) Although the manufacturers of electrical and electronic equipment are obligated to also safeguard their products against stray incoming electromagnetic interference, this is not necessarily possible for each and every given situation. This is particularly the case when older equipment is in use. The equipment is still fully capable of fulfilling its intended purpose in accord with the usual safety requirements, but an effective shielding against incoming intereference is not always possible.

As an example, fire alarms have been set off several times by mobile phones on board of airplanes. It has also occurred that the electronic control systems for automating the take-off phase have been shifted into operational situations which could have resulted in abnormal flight behaviour leading to a crash. A test conducted afterward in a flight simulator using an activated electronic control system resulted in the airplane landing next to the runway.
The German Federal Minister of Transportation Wissman has therefore initiated a legislation which forbids the use of mobile phones on board of airplanes. Disregarding the ruling could then be punished by a prison term of up to two years.

In the medical field, the danger stemming from mobile phones was already recognized in 1995. The German Federal Minister of Health Seehofer had written in a press release all the way back in the beginning of ‘95 that mobile phones could interfere with medical-technical products whose function or monitoring is based on electronic component parts. There had been reports of disruptive interference with pacemakers, pharmaceutical drug and infusion pumps, dialysis machines, artificial respirators and patient monitoring devices. With analysis equipment, it is feasible for example that an incorrect judgment or diagnosis of a person’s illness or health be made based on faulty analysis results. These, in turn, lead to the wrong treatment.

It has been observed in automotive vehicles that the use of mobile phones without an external antenna has triggered the release of airbags or prompted the failure of ABS brake systems.

unauthorized transferral of data

All of the fundamental data belonging to an industrial enterprise is stored electronically by means of a PC or mainframe computer these days, whether it’s production data, development documentation, patents, design drawings or client/supplier files.

nes

That data can be called up quite easily and inconspicuously on-site by someone who knows what he is doing. The stored information can be transferred simply and within seconds per wireless transmission by means of a mobile phone with modem, a unit which can be obtained as a standard accessory in any telephone shop. The data throughputrate is so fast that the information contained in more than 30 pages of manuscript (e.g. German DIN A4) can be transferred in less than a minute to anywhere in the world one desires. This form of industrial espionage will develop itself into one of the most effective and therefore dangerous methods in existence - if it hasn't already.

bugging and the transmission of confidential conversation

Programming mobile phones for a continuous transmitting mode can be done without any particular problems, and can be done so that the transmitting status is not recognizable outside the phone itself. A mobile phone which has been innocently placed on the table and appears to be switched off is still able to transmit every word said. The microphones within mobile phones have become so sensitive that even a telephone hidden in the room is capable of transmitting conversations with a high degree of audio quality.

The damage which could occur thereby is considerable, ranging from enormous financial losses, e.g. through stock exchange information, all the way to endangering the lives of persons in the crime-prevention sector.

The danger of both unauthorized data transmission and of electronic eavesdropping is naturally present with analog C-Net telephones as well, at least in principle. However, these units are considerably larger and therefore more conspicuous than the digital mobile phones, which tends to make using them in this sector less of a probability.

Protection against unauthorized use of mobile phones

Metal detectors are often used at airports as one possibility for locating mobile phones. They are a sure method of detecting them, allowing the phones to be switched off or taken into custody during the time spent in a security area. The draw-back is that this procedure costs a great deal of time, and therefore money, which makes it the least practicable solution most of the time. Another possibility is to monitor the ban on mobile phones with the aid of electronic detectors.

This method too presents problems of its own. As these types of situations will call for a reaction on the part of personnel, a nearly 100% guarantee for a correct detection of mobile phones must be assured. Error quotas must be so low that they are almost nonexistent.

This does present problems, because a mobile telephone in the standby mode only has a very low emission of its own. It's practically not more than that of an electrical alarm clock. The reason behind this is that customers want the standby capacity for portable communication equipment to be as long as possible. It has become a considerable advertising factor in choosing a mobile phone. Transmission time costs current and is therefore to be avoided.

Another reason for avoiding the transmission mode other than when one is placing a call is in the interests of the network's operator. Charges can only be made for calls made, not for status reports.

The standardization of the GSM Standard (the norm for mobile digital telephones) has led to the capacities of the networks being smaller than anticipated. For example, there are only 124 channels available in the D-Net. If one subtracts several of them for administration and for safety margins, the remaining total is approx. 115 channels. In Germany these remaining channels are distributed between two network operators (D1 and D2). Each supplier has therefore merely 57 radio-wave channels available to them. Eight subscribers are able to telephone simultaneously on each of the respective radio channels. This results in a maximum of 456 simultaneous phone calls per cell, in other words a restricted capacity within an area which has a minimum of 250 m and a maximum of 35 km. In reality the whole situation is reduced even more drastically because no channel overlapping is allowed to take place in neighbouring cells in order to avoid disturbances. This is the reason why the network operators also refrain from making any frequent electronic requests for status reports or up-dates from units which are logged on. In any case, the GSM standard only requires that this be done every 23 hours.

In practice, it's common in Germany that status reports are usually given every 5 to 6 hours, but not more often than that. Contrary to the widespread opinion, a mobile telephone thereby "checks in" very rarely outside of those times when a conversation is taking place. Above and beyond that, a mobile phone only transmits by itself when it changes cells, for instance while driving in a car, when logging on, when one turns the unit off and of course while dialing or talking.

In practice, detecting a mobile phone by using detectors to look for it when it is not transmitting but nonetheless switched-on (standby mode) is nearly impossible.

The best approach to the solution would naturally be to force a mobile phone to continuously transmit (e.g. status reports) by some type of auxiliary technical means. This has been regulated by law in the Netherlands, where the network operator is forced to request a status report once a minute from a mobile phone which is switched on. A ruling of this type has not been discussed yet in Germany.

An alternative to this would be “artificial” base stations which would take over this function when applied in the relevant sectors. This idea however collides with existing German telecommunication law. The BAPT (Federal Bureau for Postal Services and Telecommunication) has allocated the available frequencies to the network operators on an exclusive basis. Anyone else using these frequencies must reckon with a prison sentence of up to 2 years.

Another problem presented by this type of solution is the duration of such cognition via artificial base stations. The location process itself takes between 20 seconds and a minute due to the updating times stipulated by the GSM norm which, in turn, are effected by every mobile phone.

Narrowing down the problem, entrance filters which control access similar to those used for people at airports are unfeasible because the person in question would have to be located within a limited area for the entire identification time span.

Nevertheless, feverish efforts are being made toward finding appropriate solutions, for instance toward controlling luggage at airports which has been checked in. Problems of a legal nature require that the range of such systems be limited to circa 10 to 20 m, if and when such systems are feasible at all.

That which remains realistic today is to use detectors for detecting mobile phones in the transmitting mode (call connection time, call itself, location update, logging on, switching off phases).

Such detectors are already available in different variations on the market, whereby almost all of the equipment being offered merely monitors the frequency range in which mobile phones transmit. When looking once again at the already stated demand for “freedom” from false alarms, this option is far from sufficient. There are an extremely large number of electronic devices which also emit interference waves radiating within these frequencies and thereby inevitably lead to false alarms. Examples of such units are transponder systems as used for both automatic landing approaches in airplanes and in personal access controls, microwave units, CD players or piezoelectrical lighters.

Devices such as mobifinder® offer a viable alternative to these detectors. It is currently being used actively by well-known airlines, in many official German and Dutch agencies dealing with security, at nuclear power plants and a number of chemical plant operations. The factor here is to go beyond a monitoring of the frequency range, to closely analyse the signal received as to its structure and thereby have the ability to eliminate false alarms.

As a result, these devices consciously limit themselves to detecting digital mobile phones. An analysis of this type offering the same high degree of effectiveness is just not possible with analog units (C-Net). It does however present a far-reaching solution in view of the described dangers already being posed. Even though they are not able to completely stop the unauthorized use of mobile telephones, their use will most certainly be detected, opening the way for those means of punishment designed to enforce the ban (injunctions against trespassing all the way to criminal prosecution).

mobile telephones

modern means of communication or source of uncalculated risks?

The benefits of mobile phones and the luxurious features they offer in the world of modern communications are undisputed. The sales figures for these devices offer more than ample proof of that fact.

Be that as it may, equally undisputed are the dangers which arise from the use/abuse of mobile phones, whether unknowingly or intentional. It cannot be permitted that the price for freedom of communication be paid by innocent bystanders. In keeping with this line of thought, the confidentiality of the spoken word must also be guaranteed.

The dangers can only then be reduced to a minimum using the technical and organizational means available when the capability of an assured detection, siting and identification of switched-on mobile phones exists.

www.mobifinder.de