Protection against listening vs. information leakage channels

Lehallgatás elleni védelem vs. információszivárgási-csatornák

DOMJÁN András[1]

Abstract

Today, the press deals relatively frequently with the subject of interception, which can be approached from various perspectives. On the one hand, the focus was on obtaining information to enforce law enforcement interests, and on the other hand, so-called unauthorized, illegal observations were featured in the media. Protection against eavesdropping interacts with the need to obtain information on an ongoing basis, whether or not it is carried out unlawfully in a manner permitted by law or in the absence thereof. This dynamic phenomenon can be observed in our living environment as well as in the case of corporate, public or government buildings. Interception protection and information leakage channels are fairly closely related concepts that need to be addressed in a same system. In the following, I will describe these two areas based on their interaction.

Keywords

eavesdropping, information leakage channel, information protection, security awareness

Absztrakt

Manapság a sajtó viszonylag sűrűn foglalkozik a lehallgatás témakörével, amelyet különböző aspektusokból közelíthetünk meg. Egyfelől a bűnüldözési érdekek érvényesítése miatt alkalmazott információszerzések kerültek a fókuszba, másfelől pedig az úgynevezett engedély nélküli, illegális megfigyelések szerepeltek a médiában. A lehallgatás elleni védelem folyamatos kölcsönhatásban van az információszerzési igénnyel, függetlenül attól, hogy azt a törvény által engedélyezett módon vagy annak hiányában törvénytelenül végzik. Ez a dinamikus jelenség megfigyelhető a lakókörnyezetünkben ugyan úgy, mint a vállalati-, köz-, vagy kormányzati épületek esetében. A lehallgatás elleni védelem és az információszivárgási csatornák meglehetősen szorosan összefüggő fogalmak, amelyeket egy rendszerben kezelve kell vizsgálnunk. A következőkben ezt a két területet az egymásra gyakorolt hatásuk alapján, a közvetlen környezetünk és az objektumvédelem szemszögéből ismertetem.

Kulcsszavak

lehallgatás, információszivárgási csatorna, információvédelem, biztonságtudatosság

[1] andras.domjan@gmail.com | ORCID: 0000-0002-0178-5263 | head of department, Counter Terrorism Centre Head of Information Protection Department | osztályvezető, Terrorelhárítási Központ Információvédelmi Osztály

INFORMATION PROTECTION IN GENERAL

Nowadays, the acquisition, use, or attack of various “sensitive” information can have an impact on politics, economic actors, or even public administration. These phenomena are closely linked to informing and, where appropriate, influencing the public, freedom of the press itself and, last but not least, human rights issues. The functioning of today's modern social communication and the development of related expression habits can in some cases result in difficult-to-predict consequences. The information-sharing dumping that appears here also provides an opportunity for individuals to disclose sensitive information. There is more and more talk in the economic and industrial fields about the so-called industrial espionage, the acquisition of protected data related to product development and company strategy. As a result of technological advances, more and more professional covert surveillance tools are becoming available to everyone in the market, creating the opportunity to increase the number of secret data mining activities. Although this type of act is legal only under strict legal conditions, its trade has evolved into a fairly thriving industry through online webshops. The possibility of obtaining hidden information is given in the same way in the private sector as in the industrial environment, or even in government areas. Because of the increase in these risks, it is imperative for companies to develop their own security strategy to implement information protection.

Particular emphasis should also be placed on the training and education of individuals in this process. Interception protection and information leakage channels are both part of a larger set called the Information Security field. In the classic sense, telephone tapping is now a controlled connection to a complex infocommunication system, as both the mobile telephone network and landline telephone lines provide connections via digital exchanges.

In terms of industrial and corporate security, there is an increasing emphasis on information security and, in particular, protection against eavesdropping. The importance of the field is also proved by the fact that a separate series of standards deals with the topic under the number MSZ ISO / IEC 27001: 20xx[2]. The 2014 release is currently available with newer modifications. The standard deals with the establishment, implementation, continuous monitoring and definition of development requirements for Information Security Management Systems. It sets standards for government, commercial and non-profit organizations regarding their information systems to increase security, data protection and availability. The information security management system is based on the so-called PDCA[3] model. This allows us to continuously monitor and analyze the risks and then optimize our security system to achieve the appropriate level of protection. [1] After describing the main areas of information security, I present the concept of “eavesdropping”, starting from the risks in our everyday life, the challenges and tasks to be solved in the field of corporate and related objects protection.

[2] Information technology — Security techniques — Information security management systems. Requirements MSZ ISO/IEC Hungarian National Standard

[3] Plan-Do-Check-Act

FIELDS OF INFORMATION SECURITY

In order to guarantee confidentiality, integrity and availability, the data or information to be protected shall not be accessed by unauthorized persons, in any form, from personal security to document security to electronic information security. Accordingly, we can distinguish between physical, personal, documentary, and electronic information security based on access to information. [2]

In order to protect the information to be protected and to prevent access to infocommunication systems, it is necessary to develop a complex security measures process, together with the associated technical equipment. Physical security includes all mechanical and security protection solutions, architectural and structural designs that are able to guarantee controlled access to the protected area, the infocommunication system and the data itself. In the case of highly protected objects, great emphasis is placed on adequate physical security, primarily due to the construction of protection against explosion. In addition to the reinforcement of the building, the nearby surroundings must be coordinated with the object in order to maintain the necessary safety distances.

The scope of personal security includes the right to access classified information and to know its content at a certain level. The authorization process for access to confidential data should be preceded by a national security "screening" to identify potential risks. Continuous monitoring and multi-step access can reduce information leakage.

Document security is closely related to personal security, as the data and documents that contain the information to be protected are classified into different levels of classification, which determines the conditions under which they can be accessed and their contents known.

Electronic information security (INFOSEC) represents the infocommunication system (ICT[4]) itself, its network elements, terminals, its operational characteristics, rules, installation requirements and its impact on the environment.

Areas of electronic information security [3]:

- Transmission Security - TRANSEC
- Emanations Security - EMSEC
- Cryptographic Security - CRYPTOSEC
- Computer Security - COMPSEC
- Network Security – NETSEC

It follows from the territorial division that the equipment building the information network, the transmission media and the regulations necessary for their operation are all organized into separate groups, together with the related information protection regulations.

INFORMATION LEAKAGE - CHANNELS

The presentation of the areas of information security is a good example of how complex a system should be built, operated in a coordinated manner, and protected from

[4] Infocommunication technology

possible external "harmful" influences. In this complex system, the information leakage channels represent the set of equipment and other technical solutions that enable the transmission, radiance, connections or display of the data to be obtained. We can identify two forms depending on the type of human behavior required to obtain the information. This can be a targeted activity aimed directly at obtaining information, this is called an act of active or some kind of omission or negligence, which allows access to data, this is called a passive leakage channel. In practice, we can encounter it in the following ways.

Active information leakage channel

In order to obtain the information to be targeted, the perpetrator performs a deliberate act by extracting from the infocommunication system himself the oral speech, the events and the written materials, or the appropriate information obtained in the nearby vicinity of the target person or company and record or transmit without consent. This type of activity is illegal, only allowed to the secret services and the police, subject to strict legal conditions, for a specified period of time. Nevertheless, the industry is booming thanks to e-commerce, with virtually the capabilities of professional eavesdropping devices available for purchase without a license.

I would like to note here that in Hungary these products can be classified as "secret service equipment"[5] and their application falls within the scope of military technical activities. It is also illegal to make a statement or make a false statement about a fact that was not made during the procurement procedure, usually during the customs procedure.

Passive information leakage channel

This category includes all electronic devices, equipment, systems capable of transmitting sound, images and data, which, due to their normal or, where appropriate, different operation, provide an opportunity to get to know some or even all of the information.

In order to maintain an adequate level of information security, it is necessary to detect and continuously monitor information leakage channels and, if possible, to eliminate them. Given the complexity of the process, this type of "countermeasure" necessitates the development of a complex system of protection. Protection against interception (TSCM[6]) and eavesdropping are an integral part of security measures.

EAVESDROPPING PROTECTION

Eavesdropping protection as an activity in the field of information security cannot be linked to a single area, but rather to information leakage channels. Examining the concept literally, eavesdropping as an objective verb according to the interpretive dictionary of the Hungarian language: „*A telephone conversation is listened to and interrogated by a person who is on the line without the knowledge of the speakers.*"[7].

[5] 156/2017. (VI. 16.) Government decree on detailed rules for the authorisation of military technical activities and the certification of enterprises, XXVI. Chapter

[6] Technical Surveillance Countermeasure

[7] https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/l-39E16/lehallgat-3AECA/

Protection against eavesdropping is no longer to be taken literally, as the human voice itself is coded in a significant part of infocommunication technologies or as part of an application. The human thought itself can be considered as the starting point of the sound, data and other information that is the subject of the activity. At the present state of the art, it is not yet possible to display this with any equipment. Experiments are already underway in this area and with surprisingly good results, which means that Dutch and German researchers have been able to display the frames imaged by the human brain while watching a movie. This process was solved with a software called Brain2Pix, which put together the image seen from the fMRI[8] signals. [4] We do not yet have to reckon with this type of interception device in terms of information protection, but a similar technological process is taking place, even in the case of converting speech into an electrical signal. This is important for detection because sound, as an acoustic signal, propagates through its environment, even indirectly. Due to the complexity of the infocommunication systems, the interception cannot be handled from a purely human or technical point of view, as the joint involvement of the two areas is necessary for the realization of the act.

In connection with wiretapping, I only deal with illegal acts, I do not cover the collection of hidden audio and video information that falls within the remit of the secret services. The rather varied repository of commercially available “bugs” allows covert observations to be made as described above, creating an active channel for information leakage. In this field, the secret observation and eavesdropping is usually supported by the fact that in our everyday life and environment, technical inspection is not typical as a preventive activity. In addition to the intrusion detection system, a well-established network of cameras can be effective in terms of protection so that no spy devices in our apartment are “forgotten”, as they must somehow be introduced first in order to achieve the desired goal. However, the passive information leakage channels created by the equipment we operate can be a much bigger problem in everyday life. Of these, I would mention the breath monitors and the baby monitors, which are audio and video transmission devices designed with wireless transmission, most of which also have a speaker, which is practically suitable for two-way communication. Depending on the method of radio transmission, unauthorized persons have the option of displaying the signal available on the air with a suitable receiver. One such incident occurred in 2013 in Houston, USA, when a couple heard suspicious noises from their 2-year-old girl’s room after washing their dishes after a birthday dinner. Entering the room, a man woke their child through the baby monitor with obscene words. As it turned out, the camera device was connected to the internet on the wifi without adequate protection, so the stranger was able to access the camera. [5] In the case of analogue or digital RF cameras, depending on the sensitivity of the receiver, it is possible to obtain information by approaching the residential property.

Cameras installed in homes for security purposes can also pose a threat, as various software vulnerabilities allow hackers to gain access to our private lives as well. This happened in 2020 when a group of hackers claimed to have gained access to 50,000 home cameras and began selling their recordings online. [6]

[8] functional Magnetic Resonance Imaging

POSSIBILITIES OF LISTENING PROTECTION IN THE FIELD OF OBJECT PROTECTION

Protection against eavesdropping as part of information protection already faces serious challenges in business. Based on the risk assessment, the areas and processes of vulnerability can be identified, if possible, the possible channels of information leakage, and then the security measures can be determined. Information security can only be guaranteed by building a complex object protection system. The most critical component of the information protection measures developed as part of the facility insurance can be considered the people working there and the people visiting it, as the lack of appropriate knowledge can pose a serious risk. Unlike privacy, there is already a complex interaction between the human factor and the information security system in the area of corporate security. Personnel operating security equipment must be provided with ongoing training on current risks and their effects on security systems. Complex object protection systems can be basically divided into active and passive components.

Active protection solutions

We need different technical and tactical components to detect and prevent information leakage channels. We can be the first to consider regime measures related to properly controlled and enforced information security. This includes the introduction and use of flash drivers and any wireless equipment at the workplace. As part of our audit of TSCM activity, we are faced with the issue of confidentiality, should the company have its own technical review team if it does not have its own technical review team? This can be a headache in many cases, but it should not be forgotten that the use of instruments in reconnaissance is a rather expensive risk to the use of rather expensive devices, without them or with weaker parameters. The active category includes so-called RF monitor systems that continuously monitor of the radio spectrum. Building this type of protection is quite complicated, but it is the best solution in terms of its effectiveness. The spectrum analysis used as part of the technical review can only provide real frequency data to the operator for a short period of time, for the duration of the TSCM. Monitoring of the continuous frequency range is essential for the detection of "store and forward" type interception devices and should therefore be considered as part of effective information protection systems. In many cases, RF jammers known from military applications are recommended as protection against eavesdropping devices using radio transmission, which is a separately licensed activity.

In my opinion, in our basically crowded radio frequency environment, it is not considered to be the most efficient concept, as digital transmission technology is in many cases optimized for interference protection, so as a positive feedback it means a continuous increase in RF power, practically creating a micro oven around us. Due to the acoustic characteristics mentioned earlier, interfering devices, so-called white noise generators, are also used in the sound range, which can overdrive electroacoustic equipment and make it unsuitable for conversion (digitization). Various vibration generators are recommended for the protection of doors and windows, room partition and space dividers, in order to provide protection against contact microphones.

Passive protection solutions

In this category we can consider primarily the structural designs of the parts of the object to be protected, which are able to reduce the efficiency of the various transmission methods or even make the connection impossible. Examples include the need for RF shielding techniques using the Faraday cage principle and the need to create so-called protected negotiators. In many cases, it is not feasible to implement an “tin box” type office, but various wallpaper-like conductive materials (copper and carbon fiber coverings) and films with significant RF attenuation to protect the windows are available on the market. The combined use of these can provide up to 40 dB attenuation for protection, which can degrade the signal-to-noise ratio under certain power conditions to such an extent that a hidden eavesdropping device with wireless transmission cannot be operated. In some cases, the location of the office, such as being designed for the basement, taking advantage of the “beneficial” effect of reinforced concrete structures, has already significantly increased the security of the room.

In many cases, the security methods and designs described above are not fully implemented in practice, and information security incidents may occur. We have recently witnessed such a case in connection with a data leak in Vigadó, Budapest. In 2017, V4s and Israel held talks on a wave of refugees when, following a private discussion through the interpreter system, the Israeli prime minister shared his personal views. At the same time, members of the press were admitted to the room designated for them, where they also had access to the same interpreting system as the meeting. This was recorded by one of the participants and shared on the international news portal. [7]

IR transmission was used in this situation, but due to the organizational problem, a data leak still occurred. The source of similar problems could be audio equipment using RF connections, or so-called micro ports used for voice transmission if they do not include an encryption algorythm.

INFORMATION PROTECTION IN EVERYDAY LIFE

Due to technical progress, the infocommunication equipment we usually use, due to its complexity, is closely related to our daily activities and habits, and possibly to our interests. The resulting information can be stored in digital form or transmitted in real time via the available communication channel. This is where leaks caused by wearable devices occur, which can indirectly become an operator of an information leakage channel. As a result of uploading data from a fitness class using bluetooth technology to a server, the results of which were shared and made visible on a map, a map of Singapore’s secret military base emerged. [8] Our infocommunication equipment, our objects of use, are typically devices supported by continuous software updates, which are provided by the developers at regular intervals. The new version reaches the users after detecting the errors and vulnerabilities of the applications and then fixing them. In the event that someone does not perform these proposed updates, in some cases, there is a serious information security risk, creating an opportunity to establish information leakage channels.

In the spirit of "Connecting World," the explosive spread of IoT[9] technology in our everyday devices and environments provides new opportunities for hackers to discover and exploit information security vulnerabilities. Sensors and data transmitters, built on a myriad of wireless connections, generate traffic in the radio spectrum that can only be detected and filtered out with software with serious analytical capabilities.

SUMMARY

Taking into account the complexity of Information Security, it can be stated that it is only possible to create and operate efficiently functioning security systems in a complex way, taking into account the human factor. In addition to the personnel handling the surveillance systems, the safety-conscious behavior of individuals using electronic infocommunication equipment is also required to achieve the desired result. The average user needs a degree of self-control so that he or she does not have to connect step-by-step to all open Wi-Fi hotspots and keeps his or her software up-to-date. To achieve this, training and education are required at regular intervals for users to maintain an adequate level of protection for their own devices in addition to corporate infocommunication equipment. From the description of eavesdropping protection related to object protection, it can be seen that the classic "bug search" is not a sufficient tactical element to ensure complete security. In addition to the TSCM activity performed by specially trained professionals, a permanent RF monitor system, operated with software with appropriate processing capabilities, can guarantee the desired level of security.

LITERATURE

[1] MSZ ISO IEC 27001, „Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények," MAGYAR SZABVÁNYÜGYI TESTÜLET, 2014.

[2] Dr. Haig Zsolt, „Hadmérnök," 22. November 2006. [Online]. Available: http://www.hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.html. [Hozzáférés dátuma: 15. 10. 2018.].

[3] Várhegyi István, Haig Zsolt, Hadviselés az információs hadszíntéren, Budapest: Zrínyi Kiadó, 2005.

[4] „BITPORT," 03. 04. 2021. [Online]. Available: https://bitport.hu/kivetitettek-hogy-mit-lat-az-agy-kelloen-horrorisztikus. [Hozzáférés dátuma: 08. 10. 2021.].

[5] Alana Abramson, „abcnews.go," 13. 08. 2013. [Online]. Available: https://abcnews.go.com/blogs/headlines/2013/08/baby-monitor-hacking-alarms-houston-parents/. [Hozzáférés dátuma: 11. 10. 2020.].

[6] Szabó Dániel, „napi.hu," 22. 10. 2020. [Online]. Available: https://www.napi.hu/tech/kamera-biztonsagi-kamera-adatlopas-hacker.716124.html. [Hozzáférés dátuma: 14. 02. 2021.].

[7] hvg, „hvg.hu," 19. 07. 2017. [Online]. Available: https://hvg.hu/itthon/20170719_Bekapcsolva_maradt_Netanjahu_mikrofonja_Budapesten_ahogy_az_EUt_szidta. [Hozzáférés dátuma: 21. 07. 2017.].

[8] Rob Cyrill, „telegraph.co.uk," 18. 01. 2018. [Online]. Available: https://www.telegraph.co.uk/news/2018/01/28/fitness-tracker-data-reveal-locations-military-bases-personnel/. [Hozzáférés dátuma: 15. 04. 2019.].

[9] Internet of things