Matej Kovačič

CRASH COURSE ON CYBERSECURITY

A manual for surviving in a networked world

University of Nova Gorica Press | 2022

UNIVERSITY OF NOVA GORICA

Matej Kovačič

CRASH COURSE
ON CYBERSECURITY

A manual for surviving in a networked world

University of Nova Gorica Press | 2022

Title: Crash course on cybersecurity.
A manual for surviving in a networked world

Author: KOVAČIČ, Matej, 1974-

Reviewed by: Luis Landeiro Ribeiro, dr. Uroš Svete

Language review: Alkimist, prevajalske storitve d.o.o.

Cover design and typeset by: Birografika BORI d.o.o.

Published by: University of Nova Gorica Press,
Vipavska 13, SI-5000 Nova Gorica, Slovenia

Publication year: 2022

Online edition

Published in: PDF
http://www.ung.si/sl/zalozba/
http://www.ung.si/en/publisher/
17. 08. 2022

ISBN: 978-961-7025-24-8

Free e-publication.
Publication is founded from public resources.

Katatožni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID 116823555

ISBN 978-961-7025-24-8 (PDF)

The book was published as a part of CyberSANE project. The CyberSANE project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833683.

The publication of the book was co-financed by the Jozef Stefan Institute.

Весна

About the book

The aim of this handbook is to provide a clear overview of the various aspects of cybersecurity that are relevant for business entities and to provide technologically neutral advice for the implementation of protection against cyber-attacks within companies.

This handbook is intended for managers who are primarily responsible for the implementation of information security solutions in their business environment and for users of information technology. The provision of information security requires both technology and appropriate organisational rules (security policies). An important part of the provision of information security in an organisation is also the education of users (employees). Employees who are not aware of the security risks for the organisation represent a major hazard and poor information security can ultimately jeopardise the very existence of the organisation.

About the author

Matej Kovacic, PhD, is from Slovenia, Europe and works as a researcher at *Jozef Stefan Institute* (https://www.ijs.si/) and *International Research Centre on Artificial Intelligence* (https://ircai.org/). He is also a Senior Lecturer in Information Security at the *University of Nova Gorica* (https://www.ung.si).

He has done several presentations on cryptography and information security (especially in the area of mobile communications security) and has extensive knowledge on IT law related issues. He has experience in digital forensic analysis and is a member of expert's council of *Institute for forensics of information technology* (IFIT – http://www.ifit.si/). Personal website and blog (mostly in Slovenian language): https://telefoncek.si.

Contents

Introduction 9

Taxonomy of cyber-threats 11

Main intentional threats to cybersecurity assets 15

- Physical access 15
- Network attacks 18
- Gathering information in the cyberspace 18
- User-based attacks 20

Actors who perform cyber-attacks 24

Information system security basics 29

- Basic approaches to providing information security 29
- Provision of network security 31
- Passwords 32
  - Creating a secure password 34
  - Typical errors when using passwords 39
  - Changing passwords 41
  - Password management systems 41
  - Advanced authentication systems 42
  - Shared secrets 43
- Physical security 45
  - Tempest attack 49
- Backup 52
- Encryption 55
  - Transport-level encryption and end-to-end encryption 57
  - Man-in-the-middle attack 58
  - Encryption of email and internet communications 61
  - Encryption of mobile communications 63

Encryption of data media 65

Wiping data 66

VPN networks 68

Availability 73

Remote work 74

Anonymisation 76

Conclusion **79**

List of acronyms **80**

References **84**

Introduction

Information security involves the defence and protection of data, information systems and the entire information environment against unauthorised or unlawful access; use, disclosure, interference, modification or destruction. Information security helps us to mitigate these risks and their consequences. The goal of information security is to ensure confidentiality, authenticity, integrity and availability of data, regardless of their format: electronic, printed or any other. Cyber security covers a broader scope; it is defined as the ability to defend, protect and secure a cyber-space (the global information environment, formed by electronic communication networks and computer systems) against cyber-threats, incidents and cyber-attacks.

The field of information security has become increasingly important in recent years, both in the public and private sectors. Since the modern business environment is largely digital, it is necessary to ensure that business information and other data are protected and that the information environment is secured. Information security is not only necessary to ensure compliance with regulations and legislation (GDPR, etc.), protect the intellectual property of an organisation and to maintain a competitive advantage. It is also important because the level of information security will often influence the operations or even existence of the company. A properly regulated area of information security provides risk management and business reliability for organisations, however an equilibrium must be found between risk management and productivity.

Overall, it must be kept in mind that security is not just technology or a product or a service that is procured, but a process. The provision of information security involves both technology and people.

It cannot be guaranteed by simply purchasing suitable security equipment – it requires a strategic approach and must be managed comprehensively. The provision of information security is therefore a continuous process including organisational and technical measures to protect data or information and information systems as well to educate people (i.e. employees and users). Education is one of the most important parts of information security in an organisation, but it is often overlooked at the expense of automated technical solutions. Although the technical solutions for automating information security are certainly important, automated systems cannot completely replace IT (information technology) administrators in companies and cannot resolve all user errors.

A security culture must be developed and grown continuously, whereby we can draw an analogy from traffic safety – the safety of participants on the road depends not only on a successfully completed driver's exam; the knowledge about safety must be constantly renewed and applied.

The provision of information security therefore starts with the information infrastructure itself and continues with the protection of devices, data and applications. Users are also of utmost importance, as they are often the most exposed link in cyber-attacks. In addition to adequate protection of the final users and their devices, education must be provided as well, since employees who are not aware of the security risks for the organisation represent a major hazard.

Additionally, security mechanisms must comply with regulatory and legal requirements and support operational requirements.

Taxonomy of cyber-threats

Cyber-threats and cyber-attacks can vary considerably in a technical sense, with new forms of attacks constantly emerging. Therefore it can be difficult to establish a complete map of the attacks, since the area is always evolving. On the other hand, we must also consider threat actors with different intents, objectives and strategies to breach the protection of data and systems.

However, cyber-threats have certain characteristics that enable their classification into different subgroups. In the past years, several cyber-threats classification systems (also known as threat taxonomies) were introduced.

The European Union Agency for Network and Security Information (ENISA) threat taxonomy defines the following threats (ENISA, 2016):

- **physical attacks** (fraud, sabotage, vandalism, theft, information leakage/sharing, unauthorised physical access (entry to premises), coercion, extortion or corruption, damage from the warfare and terrorist attacks);
- **unintentional damage or loss of information or IT assets** (information leakage or sharing due to human error, erroneous use or administration of devices and systems, using information from an unreliable source, unintentional change of data in an information system, inadequate design and planning or improperly adaptation, damage caused by a third party, damages resulting from penetration testing, loss of information in the cloud, loss of (integrity of) sensitive information, loss of devices, storage media and documents, destruction of records);
- **disasters** (natural and human caused disasters);

- **failures and malfunctions** (of devices or systems, disruption of communication links, main supply, service providers (supply chain) and malfunction of equipment);
- **outages** (loss of resources, absence of personnel, loss of support services, internet or network outage);
- **eavesdropping, interception or hijacking** (wardriving, intercepting compromising emissions, interception of information, interfering radiation, replay of messages, network reconnaissance, network traffic manipulation and information gathering, man in the middle attacks);
- **nefarious activity or abuse** (identity theft, spam mail, denial of service, malware, social engineering, abuse of information leakage, generation and use of rogue certificates, manipulation of hardware and software, manipulation of information, misuse of audit tools, information and information systems, unauthorised activities (including unauthorised installation of software, data breaches, hoaxes, remote activities (execution), targeted attacks (APTs etc.), failed of business process, brute force and abuse of authorisations);
- **legal** (violation of laws or regulations, failure to meet contractual requirements, unauthorised use of IPR protected resources, abuse of personal data, judiciary decisions/court orders).

We can see that ENISA’s classification includes cyber and non-cyber-threats, human and non-human induced threats and that threats could be intentional or accidental.

However, as we already mentioned, security is not just about technology. It also involves people and sometimes even the broader environment (threats from human and non-human events in the environment).

If we focus to people and technology, cyber-threats could therefore be classified into four main groups:

- **Loss of assets** because of disasters, failures, damage, malfunctions and outages. These threats could be accidental or intentional (for instance, denial of service attacks).
- **Cyber-attacks to the systems and data.** Some of them require physical access to the systems, while others could be performed with network access (for instance several attacks on communications, like intercepting or manipulation of network traffic as well as direct attacks on "virtual space"), exploiting human errors, mistakes by administration of devices and systems, 0-day vulnerabilities, etc.
- **Network reconnaissance and information gathering.** It also includes information leakage due to human errors or lack of knowledge (for instance information mistakenly published on the internet).
- **User-based attacks**. These include all cases where users of information technology are manipulated, for instance with social engineering, hoaxes but also extortion or corruption, cases where users are subject to identity and/or credentials theft or information leakage and cases where users are intentionally taking activities like sabotage, vandalism, theft, manipulation of hardware, software or information performing unauthorised activities.

While it is very hard to prevent all threats, in many cases these threats could be mitigated by adequate design of systems, adequate planning and education of users and administrators of these systems. This includes implementing active and passive measures for systems and information protection, including preparation of contingency plans and disaster recovery.

While some of the outlined threats are accidental/non-intentional (failures, outages, etc.), some others are intentional, which refer to purposeful actions to attack cybersecurity assets.

Main intentional threats to cybersecurity assets

In the following chapters we will outline some main intentional threats to the cybersecurity assets. These are physical access to the systems and data, network attacks (access through virtual space), gathering information in the cyberspace and user-based attacks (which is actually an indirect attack on cybersecurity assets through people).

Physical access

Physical security is a very important aspect of information system security that is neglected all too often. The purpose of physical protection of access to information systems is to prevent unauthorised access to the information system and the information contained within. This is not just an issue of theft; an attacker may use physical access to the information system to install malicious software or hardware to circumvent the existing security mechanisms or obtain remote access to the system. We should also be mindful of discarded computer components which may still contain sensitive data. This includes not only hard drives and flash drives but also mobile phones and even printers with built-in data storage and other peripheral devices.

Physical access therefore does not mean only access to premises where the cybersecurity assets are located, but a general access to them. That includes access from the point of manufacturing (this includes possibility of supply-chain interdiction,[1] i.e. intercepting equipment that is being shipped to the target customer, which could be performed by nation state actors or by cybercrime organisations), access by servicemen and all up to when equipment is discarded. Access by unauthorised personnel should also be considered, for instance visitors, cleaning service, security and other people who can access the premises where equipment is located. Those people could access the data by physically opening computer devices and copying data directly from storage media, but also by inserting USB drives to the target device, connecting other data-transfer interfaces (for instance Firewire[2] devices, USB network interfaces, so-called BadUSB devices,[3] etc.) Relevant physical access

[1] One of the first supply-chain attacks has been described in the book *At the Abyss: An Insider's History of the Cold War* by Thomas C. Reed, however it is not entirely clear whether it really happened. Reed stated that the United States discovered that the Soviet Union was stealing US technology for running gas pipelines (through Canada company), so they planted a malware to a gas pipeline control software. This software has been deployed on a Trans-Siberian gas pipeline, where it created malfunctioning of the pumps, leading to a gas explosion. However, while this seems possible, these statements have not been confirmed by US intelligence agencies and was later even denied by KGB veteran Vasily Pchelintsev, who said that gas explosion was caused by poor construction rather than sabotage (Zetter, 2014: 454). Another well known example of supply-chain attack is a Stuxnet malware, which was American-Israeli cyber weapon used to damage uranium enrichment programs by the Iran (probably developed in 2005, but discovered in 2010). One of the largest most recent supply-chain attacks is the SolarWinds attack in 2020 (also known as Global Supply Chain Cyberattack), which has been performed through the IT infrastructure company SolarWinds. It is believed to be carried out by the Russian government (however Russian government denied they have been involved), and has been probably one of the major cyber-espionage incidents that affected United States, NATO and several major US companies among others (Newman, 2021).

[2] Firewire, also called IEEE 1394 or i.LINK is a high-speed computer data-transfer interface.

[3] BadUSB is a computer security attack using USB devices that are programmed with malicious software. Usually these devices act as a human interface device (HID), such as a keyboard or mouse, and can be used to dis-

entry is also so-called boot overriding, when an attacker boots the target computer from external storage device (USB,[4] CD[5] or DVD[6]) and is then able to access the data on internal storage devices. Some data transfer interfaces, for instance Firewire, have so-called direct memory access (DMA), which enables an attacker to read and write memory off a target system directly, bypassing the operating system. By reading memory, an attacker can steal encryption keys from the target device, and by overwriting memory, attacker can bypass lock screen, modify the system or install and run malware.

Physical access can also allow an attacker to perform Cold Boot attack, which is a type of side channel attack where an attacker with physical access to a computer can perform a memory dump of a computer's random-access memory (RAM).[7] This is done by performing a hard reset of the target machine and then booting a lightweight operating system from a removable disk and then copying (dumping) the contents of RAM memory to a file. This is possible because DRAM (Dynamic random-access memory) and SRAM (Static random-access memory) are not fully volatile, so data is not completely lost when power is removed, but they remain readable a couple of seconds to minutes after the power is switched off (this time could even be extended by cooling RAM chips to a low temperature).

creetly execute commands or run malicious programs on the target device.

[4] USB stands for Universal Serial Bus.

[5] CD stands for Compact Disk, a digital optical disc data storage format.

[6] DVD stands for Digital Versatile Disc, a digital optical disc data storage format.

[7] RAM memory – Random-Access Memory is a form of computer memory that can be read and changed directly. Typically, is used to store working data and machine code.

Network attacks

Network attacks could be divided into attacks on network links and communications and attacks on so-called virtual space.

Attacks on network links and communications are including all methods and techniques of intercepting or manipulation (including redirection) of network traffic, where an attacker can gain access to the content of the communication or insert fake content into the communication between any two points.

Attacks on a virtual space (that includes unwarranted entry to the virtual space) of the user or organisation typically involves various types of intrusion or any other form of unauthorised access to the systems, for instance guessing access credentials, gaining access with unchanged default passwords, exploiting human errors and mistakes by administration of devices and systems, exploiting 0-day vulnerabilities, etc.

Gathering information in the cyberspace

Internet search engines and social networks are a valuable source of information. Attackers know that, so information gathering is usually the first step or a preparation tool for an actual attack. Some information that could be gathered are public by the nature. Typical examples are information that could be gathered by browsing internet resources, querying DNS[8] and WHOIS databases[9] and information from various official registries. This is sometimes also called open-source intelligence

[8] DNS – Domain Name System is the hierarchical and decentralised naming system that translates human readable domain names to machine readable IP addresses.

[9] WHOIS – a database which stores registered users or assignees of internet resources like domain name, IP address block or autonomous system data.

(OSINT), which is a set of strategies and methods for the collection and analysis of data gathered from publicly available sources to produce actionable intelligence. However, some information is available as a consequence of information leakage due to human errors, carelessness or lack of knowledge (typical example of the latter is the information mistakenly published on the internet).

Users often publish a lot of information on social networks; some have been doing so for several years. An analysis of this information can reveal a significant amount about the user. Internet search engines are particularly interesting, as they can also reveal hidden information. For example, files that users have erroneously stored on publicly available servers (sometimes even confidential and secret documents can be found in this way), accidentally opened access to databases as well as various devices that are inadvertently accessible to the public (e.g. webcams, printers, baby-cameras or “babycams”, routers, even industrial systems that can be remotely controlled). The analysis of metadata in publicly available documents may also reveal additional information.

Among the first to be aware of the possibilities of such information collection were members of an American hacker group *L0pht Heavy Industries*, active in the years between 1992 and 2000, who scoured public web sites of various organisations, searching for documents containing terms such as “confidential” or “password”. A security researcher from Poland, Michal Zalewski, was probably the first person who published a post (in August 2001) describing use of the search engines for attacking internet servers (Zalewski, 2001). The same year, in November, a French security researcher Vincent Gaillot demonstrated how confidential information can be searched using the Google search engine (Gaillot, 2001), and a few years later, security researchers Johnny Long and Ed Skoudis wrote a book titled *Google Hacking for Penetration Testers* on this topic (Long and Skoudis, 2005). In 2009, a specialised search engine, Shodan,[10] appeared on the internet, which could be used to find unprotected IoT[11] devices and services, and today several tools exist that can help hackers or security researchers to search for various types of internet devices and to analyse metadata in public documents.

As we can see, network reconnaissance attacks are usually the first step of an actual attack, and that kind of information gathering could be very effective while it does not require extensive technical knowledge from the attacker. Network reconnaissance attacks are usually divided into public, social and software reconnaissance attacks. In public reconnaissance attacks an attacker collects information about the target from public domains, while in software reconnaissance attacks an attacker uses special software tools to gather information about the target. These includes tools for DNS querying, network scanning, service discovery, and so on. In social reconnaissance attack the targets are humans and an attacker uses social engineering to gather information. This will be discussed in more detail in the next chapter.

User-based attacks

Social engineering describes a set of techniques that attackers use to gain benefits by manipulating or abusing an individual's trust. The attacker (also referred to as social engineer) uses social skills and psychological techniques (i.e. persuasion, de-

[10] Shodan is available at: https://www.shodan.io/.

[11] IoT – Internet of Things, physical objects that are embedded with sensors and software that connect and exchange data with other devices and systems over the communications networks.

ception, inspiring trust, exploitation of people's reactions in a certain situation) to obtain personal or sensitive information (which would then be exploited in the next phase) from the victim, to persuade the victim to take a certain course of action or to blackmail or threaten the victim. Social engineering is also often used in combination with classic "hacker" techniques (e.g. sending fake emails, redirecting to fake websites).

For example, attackers may use social engineering to convince or mislead the user to provide their email access information, and this information is then used to illegally log into the user's mail account. Subsequently, they may take on the identity of the user for further deception.

Social engineering attacks consist of four steps. In the first step, the attacker attempts to gather as much information as possible on the potential victim. This includes both personal data and data on their information environment and the organisation itself (information on suppliers, customers etc.) This data is then used by the attacker in the second phase to establish and develop a relationship with the victim. At this stage, the attacker plays a certain role (e.g. they present themselves as a computer repairer, supplier representative) and seeks to gain the trust of the victim through the provision of information or knowledge obtained during the first phase. The third phase involves the exploitation of the established trust (e.g. tricking the victim into providing confidential information), and phase four involves using the data obtained to achieve the objective pursued. At this point, the life cycle of a social engineering attack can be repeated (the attacker collects additional data or broadens the attack, uses the collected data on a second victim, etc.)

Attackers use various methods for collecting data for social engineering. The simplest way is searching for data through internet search engines and social networks, but attackers can also use phishing (an act of misleading users, in which the attacker attempts to extract personal and other sensitive information from victims using false websites[12] or emails), pharming (redirecting victims to false websites through DNS rerouting) and malware based attacks.

Some more direct approaches include social engineering by telephone (e.g. the attacker will call a company posing as a service provider or pretending to conduct a survey) and so-called vishing (voice phishing), where the attacker calls the victim by phone but modifies the call identification by replacing the real telephone number with another number (e.g. a supplier's or the true service provider's telephone number). Then there is also physical observation of the victim, so-called shoulder surfing. This can take place in public places (e.g. credit card payments, or ATM cash withdrawals) as well as in business premises (e.g. when an employee logs onto a computer). A large source of information can be found by dumpster diving or *trashing*, which includes the examination of discarded computer equipment and business documentation. Attackers may also plant infected storage media (flash drives, CD/DVD media, etc.), and there have even been cases where attackers physically broke into the company to install a backdoor to the organisation's ICT[13] infrastructure (for instance a wireless access point that enabled them access to the network, keylogger, malware, etc.)

However, users can fail security in other ways too, not just by manipulation. The problem is also carelessness, ignorance and negligence of users, not following security protocols and lack of knowledge and underdeveloped security culture. This type of social reconnaissance attacks could be reduced by education and training of users.

[12] False websites they are usually presented in a form of copycat websites with similar almost indistinguishable domain names.

[13] ICT – Information and Communications Technology is the infrastructure and components that enable modern computing.

However, a very special problem are cases where users are intentionally taking prohibited activities like sabotage, vandalism, theft, espionage, manipulation of hardware, software or information and performing unauthorised activities. A defence of insider threats in a form of rogue or disgruntled insiders (users) that are intentionally performing malicious acts is very hard and this is definitively not a problem that could be solved solely with technology. Technology (technical controls and proactive detection of abnormal user activity) and training of users definitively helps, however for mitigating these threats, approaches like long-term creation of trust and loyalty are also important.

Actors who perform cyber-attacks

Some define cybercrime as any form of crime involving computers and, more generally, information technology (IT). However, cybercrime is not only the use of information and communication technology for criminal purposes; an essential element of cybercrime is that it could not be possible without the use of technology, at least not to this extent.

Cybercrime differs from its traditional counterpart in three essential characteristics. First, it can be carried out remotely. Second, the identity of the attacker is relatively easily concealed or falsified. And third, tracking the information system that is the origin of the attack is not always possible, since attackers often employ methods like looping or weaving. In the latter, the attacker does not connect to the target system directly but through a number of other systems, possibly located in different countries, which prevents, or at least complicates, tracking them down.

The term “hacker” was coined by Joseph Weizenbaum in 1976 (Voiskounsky, Babveva and Smyslova, 2000: 57), and today it is popularly used to describe an individual possessing a lot of technical computer knowledge and using this knowledge to attack computer systems; this firmly places hackers within the realm of computer crime. Consequently, the term is presently associated with sophisticated illegal activities, although so-called “hacking” is more of a way of thinking rather than the methods employed to use these skills. White-hat hackers, or ethical hackers, who are information or network security experts, attempt to discover the shortcomings in the security of information systems of companies in a completely legal manner, using various attack methods. Ethical hackers use exactly the same methods as so-called black hat hackers, but the goal of the former is not to perform harm, but a security review and thorough analysis of the information system and to prepare recommendations to improve the security.

For organisations wishing to provide a higher level of security, it is therefore certainly reasonable to hire ethical hackers to run a security check or a penetration test (checking the organisation's security protection through simulated attack). Performing security checks on the organisation's key applications makes sense as well, and it can be performed by external or internal experts.

In some sectors, for example banking, such checks are mandatory. The internationally accepted security recommendations of the PCI-DSS (Payment Card Industry Data Standard – intended for organisations that directly or indirectly manage payment card information) provide that security checks (of different intensities) are to be carried out at least once a year or upon any major changes to the information system. The PCI-DSS standard stipulates that organisations are to conduct an internal and external vulnerability scan at least on a quarterly basis as well as thorough penetration testing following any major modification of the information system or annually.[14]

The motives of cybercriminals in the past have been often the desire for discovery and self-expression, but today, most cyber-attacks are akin to traditional crime – carried out purely for profit. Some present-day cyber-attacks are also motivated by political activism (so-called hacktivism), and there have even been cases of cyberterrorism and cyber-sabotage.

[14] PCI DSS, version 4.0 (March 2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

In recent years, we have seen the emergence of countries as actors in the field of cyber-attacks, however this is not something new. Probably one of the first documented examples of cyber-espionage was described in a book *The Cuckoo's Egg*, written by Cliff Stoll. The author of the book was managing computers at Lawrence Berkeley National Laboratory (LBNL) in California where he found out that unauthorised user was using LBNL systems to access military bases around the United States, looking for sensitive data. Stoll later found that the intrusion was coming from West Germany via satellite connection, and the following investigation found out that the group of young German hackers were selling the results of this hacking, as well as knowledge about computer system's vulnerabilities, to the KGB,[15] the Soviet Union's intelligence agency (Stoll, 1990). This means that secret services started to use cyberespionage techniques at least in 1986 or 1987.[16]

Today we are faced with an increase of information-intelligence attacks, carried out both for industrial espionage purposes and military intelligence hacking, as well as spreading political or public opinions, fake news and propaganda[17]. The fi-

[15] KGB (Komitet Gosudarstvennoy Bezopasnosti – Committee for State Security) was the main security agency for the Soviet Union.

[16] The United States is probably the country with the most digital surveillance capabilities, whose cyberespionage programmes were exposed by whistleblower and ex-CIA contractor Edward Snowden in 2013. However, cyberespionage is used by several other countries, including China, Russia, Israel, Iran, EU countries and North Korea. North Korean cyberwarfare groups are among the world's most sophisticated and are known to perform cyberattacks for intelligence collection and espionage purposes, and to finance development of nuclear weapons. In 2019 North Korea allegedly generated around 2 billion USD from ransomware campaigns, and this money has been invested in their nuclear weapons programmes (Nichols, 2019).

[17] The use of fake news and propaganda in politics and war is also not something new, only the medium on which these activities take place is new. In the past, misinformation campaigns were carried out by press, radio and TV, now internet and social media is being used. While state-spon-

nal stage in this development are cyberwarfare and cyber war,[18] the elements of which could be seen in some traditional military conflicts as early as in 2008 in the Russo-Georgian war,[19] when Russia allegedly began a cyber-attacks on the Georgian IT infrastructure (government websites, news agency and radio, some industrial infrastructure, and others).[20]

Sometimes cyberwarfare could be an initial stage of a followed armed conflict. One of the examples of this are cyber-attacks on the Ukrainian government and banking sector with wiper

sored influence of online views is practised by many countries, it seems that today's Russia has a leading role in various online misinformation campaigns. Their misinformation campaigns are carried out by so-called Russian web brigades (also called Russian trolls) operated by people and also with a help of so-called social bots, which are automated programs used to engage in social media. However, this is no surprise, since Russian state has a long tradition of these activities. Some of these activities were described in a book *Double Lives* written by *Stephen Koch*, who described how the *Soviet Union* tried to shape Western cultural opinion in the 1920's and 1930's with manipulation and propaganda through vast publishing network and interlocking front organisations under the covert direction of the *Communist International* (Comintern) and the Soviet secret services (Koch, 2004).

[18] The term war inherently refers to a large scale action, it is an actual, intentional and widespread armed conflict. Warfare refers to the activities of war in general. Cyber warfare includes techniques and tactics which may be involved in a cyber war.

[19] The Russo-Georgian war was a military conflict between Georgia, Russia and the (Russian-backed) self-proclaimed republics of South Ossetia and Abkhazia.

[20] The Russian government later denied the allegations that it was behind the attacks and stated it was possible that individuals in Russia had taken it upon themselves to start the attacks. (Markoff, 2008). However, the first-wave of cyber-attacks launched against Georgian media sites seems to be in line with military operations in Russo-Georgian war (Prince, 2009). There were also an estimates that cyber-attacks on Georgia (and also on Azerbaijan in 2008) may have been out-sourced to the Russian Business Network, cybercrime organisation from Russia (Leyden, 2009) to create plausible deniability for the Russian government.

malware[21] and DDoS[22] in February 2022, just a few hours before traditional armed attack to Ukraine (Milmo, 2022).[23]

However the entry of state actors into the field of cyber-attacks, and the use of information-intelligence attacks for industrial espionage, is of particular concern to business organisations. Thus, the provision of information security for businesses is also becoming increasingly important from a strategic viewpoint.

[21] Wiper attacks are highly destructive in nature and involve wiping data from the victim.

[22] DDoS – Distributed denial-of-service attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming with a flood of internet traffic.

[23] Cyberwarfare has been an important component of confrontation between Russia and Ukraine in the past. Russian allegedly used their cyberespionage weapons (Uroburos) since 2005, but first major attacks on Ukrainian systems were recorded during mass protests in 2013 and later: Ukraine power grid hack at in 2015 and 2016, attacks on the State Treasury of Ukraine in December 2016, a series of ransomware attacks in June 2017 (Petya malware) and attacks on Ukrainian government websites in January 2022. It should also be noted, that since 2016 Ukraine also performed cyberattacks against Russia.

Information system security basics

The provision of information security involves both technology and people (see above). It is important that we see this as a process. Technical solutions can only provide part of the solution. It is also important to adopt and implement appropriate security policies and to educate employees of basic security behaviour. Although education is one of the most important parts of information security in an organisation, it is often overlooked at the expense of automated technical solutions. In this context, it is important to remember that education must be continuous, as this is the only way for employees to acquire and maintain the appropriate competences to deal with cyber-threats, as information technology is changing rapidly and new risks and threats are emerging in the field of information security.

Below we will look at some of the most important approaches to information security within an organisation, but similar approaches can also be used in private life.

Basic approaches to providing information security

Today, the basics of information security primarily include regular software updates. This does not mean just the operating system but also all applications, software libraries and firmware on all devices, including peripherals such as Wi-Fi access points, routers, as well as phones, tablets and similar devices. This is an area where great progress has been made in recent years, with operating system manufacturers regularly releasing security updates and increasingly pushing users to keep up to date as much as possible. Whereas in the past you had to go through a lot of trouble to install security updates, today you have difficulties to avoid installing security updates.

The basic building blocks of enterprise information security include the use of anti-virus and anti-malware software, but for virtually any organisation, the use of at least basic network security is worth considering as well. In addition to antivirus software, it makes sense to install Endpoint Detection and Response (EDR) software on computers. As mentioned above, these tools are installed on endpoint devices (PCs, laptops and mobile devices), not on the network, and are designed to detect and log suspicious activity and prevent cyber-threats on these devices as well as to respond quickly to perceived potential security incidents.

It is also sensible to install applications to block online trackers[24] and so-called "junk removers" on end-user computers (these are applications which provide cleaning a computer system).[25] In order to increase privacy in the Windows environment, it is also worth considering blocking Windows telemetry.[26]

At the same time, it must not be forgotten that the preparation of appropriate security policies, also formally define security within the organisation and user rights, as well as systems for logging and monitoring compliance with established rules. This includes regular efforts to develop an appropriate security culture to equip IT administrators and users with the skills to identify cyber-attacks.

[24] Some of these applications or add-ons for web browsers are: Ghostery, Privacy Badger, Adblock Plus, uBlock Origin, Facebook Container, NoScript, etc.

[25] Bleachbit, CCleaner in Windows, Onyx in Mac, etc.

[26] Blocking Windows telemetry on the PC is possible with applications such as Blackbird, WPD, or by blocking the access to the telemetry servers directly on the network.

Provision of network security

A firewall is the most important element of protection against network attacks. In principle, the use of a firewall can only be omitted if no application or service that receives connections from the network is running on a computer or other devices on the network. In all other cases, the use of a firewall is almost always sensible, as a conventional firewall puts only a minimal load on the system.

A firewall is basically designed to separate two network segments, and the rules defined in the firewall allow or disallow communication between two network nodes or two network segments. Although the firewall is responsible for limiting network connections, we should be aware that the firewall itself does not prevent all unwanted access to a computer. Access is still possible through applications that connect to the network or services running on the computer. If, for example, files and network resources are allowed to be shared on the computer, it is logical that the firewall will allow this type of access to a computer, while other access attempts will be blocked (if set). Thus, the firewall will provide a certain level of security, but unwanted access to the computer may still be possible through the misuse of the sharing of files and network resources.

It should be emphasised that it is not necessary to start communication from the outside to perform the attack. In other words, a firewall can block all attempts to connect from the network to our computer, but this does not guarantee that an attacker will not be able to connect to a computer, because firewalls are not effective against phishing attacks, especially if they only block incoming traffic and have unrestricted outbound traffic. Even a very restrictive firewall will usually allow connections from a computer to the external network (otherwise it would not be possible to browse the web, etc.) This allows the attacker to set up a so-called reverse tunnel. An attacker can install a malicious application or send the user a web link that opens a communication channel from the victim's computer to the attacker. The attacker can then enter the victim's computer through this communication channel. Therefore, as part of network security, it makes sense to define firewall rules at the level of the individual applications.

In the context of network monitoring, it is worth to consider using tools to monitor internet usage (so-called parental controls) to block access to unwanted content (for instance pornography, phishing sites, or malware distribution sites). At network level, it makes sense to consider the use of tools for scanning (and possibly also limiting) bandwidth usage (which can detect suspicious network activity) or an IDS/IPS system (so-called Intrusion Detection/Prevention Systems – these are solutions for the detection and/or prevention of network attacks). There are many open source[27] and commercial solutions available on the market today that can enable us to protect our network against known threats in real time. There are also more advanced firewalls that use artificial intelligence (AI) or machine learning (ML) to automatically adapt the rules or levels of network security.

Passwords

Passwords are the basic and most used security mechanism, so passwords should generally be complex and long enough to provide the desired level of security. So-called "encryption keys" are similar protective mechanisms; however, they are usually longer than passwords and have more entropy as they often involve randomly generated data. Encryption keys can

[27] For instance Snort, Zeek, OSSEC, Suricata, or Security Onion.

also be stored in a file (for instance in a digital certificate) or on a special device (so-called hardware tokens).

The problem with passwords is that complex passwords are difficult to remember, so when we are creating passwords, we are faced with the dilemma of whether we want more security or easier use. In the following chapter, we will initially look at how to create appropriate (secure) passwords, the most common mistakes when creating passwords and how to save and secure them in a simple and safe manner.

We can use several methods for creating passwords, but it is important that the password is as long as possible and as complex as possible (a mixture of letters and numbers, preferably a mixture of upper- and lower-case letters and numbers). We are of course talking about important passwords, e.g. password for access to encrypted data, password for access to email. At this point, we should also mention one-time passwords – these are passwords that can only be used once, after which they expire and are no longer valid.

When creating passwords, pay attention to the fact that when entering them, we can encounter different localisation systems or different keyboard layouts. The *English Keyboard* does not contain your local language characters (for instance in Slovenian language we have characters like “č”, “š” and “ž”), and some letters on the keyboard could switched (for example, “z” and “y”), etc. When you start the system, the operating system does not yet have a default language set, so the *English Keyboard* layout is usually used at that time; entering a password containing the letter “z” may be different at start-up than later, when the system is already active.

When using passwords, it is also important to be aware of some of the security limitations of passwords. One originates from the ability of the system administrator to reset or recover the password (there are special schemes for recovering (forgotten) passwords, e.g. key escrow). Another possibility to consider is, that sometimes data could be accessed with forensic tools without a password. Password backups can exist (e.g. master key) to unlock the data. While password recovery systems are encouraged, be aware that these systems can also be abused. Which is just additional proof that security also involves people (loyalty and trust in the system administrators).

In some cases, “biometric passwords” are used to access the system. However, it is important to be aware that the use of biometric parameters for passwords is problematic, as biometric parameters cannot be changed or revoked, and there are known cases of biometric parameters being forged using relatively simple technology (e.g. fingerprint forgery). It is important that the identity (“Who are you?”) and authentication (“How can you prove it?”) of the user remain separate, which is not the case when using biometric passwords. Biometrics should therefore only be used for identification (as a substitute for a username), and the user is then authenticated with a password or key.

Creating a secure password

In the modern world it makes sense to use a special app – *a password generator* – to create a password. There are different methods available to choose a secure password. When choosing a password, it is not a good idea to choose passwords that are associated with the user or that contain dates, phone numbers or different sequences (consecutive characters, consecutive numbers or consecutive keyboard keys).

Below we will see four possible methods for creating a password (they could also be combined), but it is important that we do not use the same or similar passwords for different services. Initially, it makes sense to ask how important the password really is. If it is a password required by a web page, e.g. for downloading a file, and we will never use the password or service again, it is, of course, pointless to create a very secure password. This is completely different with passwords for access to important internet services, encrypted data or access passwords for our user accounts. Especially important are passwords that secure your source of trust. For instance, several people use personal email as the guardian for access codes and passwords. Losing access to personal email, can compromise a user in serious ways, because it allows an attacker to recover several of the user's access codes and passwords. So-called source of trust passwords therefore should require extra care, and should be complemented with two-factor authentication (2FA) or multi-factor authentication (MFA).

The first method to create a password is to construct the passphrase from a sentence, or the password is identical to a sentence. For example, we can use the sentence "This is my password". In this way, it is not too difficult to create a long enough password that can easily be remembered. We can also invent a (meaningless) sequence of words, e.g. "Mountains Sea Hill Valley". It makes sense to use numbers and other characters, but it's good to keep in mind that you may need to enter your password on a keyboard with a different character layout than the one you used to create it (e.g. one that has no characters for your local language).

The second method involves replacing certain letters in the password with numbers that visually resemble those letters. For example, "O" is replaced with the number zero, "L" with one, "A" with four, etc. Example: "th1s1smyp4ssw0rd". However, using only this method may lead to poor security of passwords, because this method is well known to attackers and can be easier to brute-force than the first method.

In the third method, the password is assembled from the first (or second, or last ...) letters of the parts of text. For example, from "One, two, sky blue, all out except you", we get "otsbaoey". Of course, other combinations are possible (e.g. a combination of words and numbers), the only important thing is that the password is long enough and complex enough to be unguessable.

The fourth method is known as *diceware*. This is a method for creating passwords using a regular dice, which serves as a random number generator. The password is made up of several words, and to select each word, the dice must be rolled five times. This gives us a 5-digit number, which returns the word to be used for the password part in a separate table.[28] The words in the tables are chosen to be easy to pronounce and easy to remember, and the word tables are available for different languages. There are 7776 words in each language table (6^5 – the dice returns values from 1 to 6, for each word the dice is rolled five times).

For example (in the case of English), "13554" returns "befall", "32425" returns "have", and "54244" returns "ski". The final password consisting of these three words would be "befallhaveski". The author of the *diceware* method, Arnold Reinhold, has recommended that the method should be used to choose a password containing at least six words.

It is important to remember that passwords must be sufficiently different from each other. For example, it does not make sense to use phrases like "This is the email password", "This is the bank password", etc. An attacker who manages to reveal the contents of one password (e.g. on a forum) can quickly guess the system used to create the passwords and thus guess all the others.

[28] The tables for the different languages are available at https://diceware.com and at the https://theworld.com/~reinhold/diceware.html.

There is very well known case of a security researcher Dan Kaminsky, whose computer was hacked in 2009 and whose passwords were later publicly disclosed. Kaminsky was using passwords created using the following system: “fuck.hackers”, “fuck.omg”, “fuck.vps”, “fuck.mysql”, etc. Once the attackers had discovered the pattern of passwords used to access a few systems, guessing the remaining passwords was much easier.

In short, passwords for access to encrypted data (e.g. encrypted disks) must be significantly different from passwords for access to less important online services and other systems.

The length of the password is important, because a password that is too short allows an effective brute force attack (guessing all possible combinations of letters and numbers) or dictionary attack (guessing passwords from dictionary words). There are a number of programs on the web that allow you to recover “forgotten” passwords, and these programs are very effective at guessing passwords that are short enough on modern computers. Password cracking can be greatly facilitated by modern GPUs (Graphics Processing Units). Graphics cards speed up password cracking by 50 to 100 times compared to conventional computers, and GPU password cracking can be parallelised (using multiple graphics cards to crack passwords in parallel). Modern graphics cards can check billions of passwords per second, and as computers evolve, the time it takes to successfully crack a password is only decreasing.

As mentioned earlier, the password should be as long as possible. The question is, what is the minimum reasonable length? The answer depends on the type of a password. If it is a password for accessing a system that has a time limit on password retries (e.g. is waiting after an incorrect password, and this waiting time may even increase for each subsequent incorrect entry) or if the number of attempts to enter the password is limited (e.g. in mobile phones, you can only try to enter the PIN three times, after which the SIM card is locked), the password can be shorter. But if the password is for access to our encrypted data that a possible attacker who physically obtains access to it will be able to try to decrypt infinitely many times, on a very fast computer, the password must of course be longer.

The quality of the password is measured by entropy (a measure for the randomness, or uncertainty of a message system). Entropy increases with the length of the password and depends on the character set used. While individual characters in the full ASCII set are considered to contain 8 bits of entropy, characters in the “normal” ASCII alphabet (upper- and lower-case letters, numbers, punctuation, etc.) are considered to have only about 5 bits of entropy. However, if you use a natural language text for the password, the password must be even longer, because the entropy of natural language is even lower due to grammar and word-building rules.

According to some estimates, English text has an average of about 1.2 bits of entropy per character (this is a conservative estimate), which means that for a really high level of security, you need a password over 54 characters long (which achieves 64 bits of entropy). The level of entropy of Slovenian literary texts was estimated by Primož Jakopin. In his book, *Entropija v slovenskih leposlovnih besedilih* (“Entropy in Slovenian literary texts”), published in 2002[29], he estimated that average entropy of Slovenian literary texts is 2.2 bits per character. It follows that a password in the Slovenian language must be at least 30 characters long to reach 64 bits of entropy. Entropy measures for different languages are different. Estimates of how much entropy a password should have vary widely. The *Network Working Group* Recommendation from 2005, “Randomness

[29] Book has been published in Slovenian language.

Requirements for Security”[30], states that passwords of low importance should have at least 29 bits of entropy, while those of high importance should have up to 96 bits of entropy. But this estimate is rather old, and some other estimates indicate even higher numbers. How the entropy is translated to password length depends on used character set. A password could be composed from numbers only or Latin alphabet, but it could also be alphanumeric (combination of alphabetical and numerical characters), case sensitive or case insensitive or even can contain some special characters (separators, etc.)

General advice would be that passwords should contain case sensitive alphanumeric and special characters and should be long at least 20 characters or more (preferably at least 32). Passwords that are very important should be even longer (45 or more characters long).[31]

It is, of course, up to the user to decide what is a reasonable password length for a given password, as passwords also have a usability component – longer passwords are harder to remember.

Typical errors when using passwords

Typical mistakes when using sufficiently long and complex passwords are not storing them properly (e.g. on sticky notes on the monitor or under the keyboard) and password recycling, i.e. using the same passwords on different systems (if an attacker manages to break into one system and steal a poorly

[30] The text of the recommendation can be found at: https://tools.ietf.org/html/rfc4086.

[31] Please note that this recommendation is valid at the time of writing this book (beginning of 2022). Due to increased computing power (better processors), longer passwords need to be used in the future.

protected password, they will gain access to more protected systems). As previously stated above, passwords for access to encrypted data must be significantly different from passwords for access to online services and other systems.

Some password recovery systems are also problematic, e.g. authentication with known data (typical examples are “security questions” that allow password recovery, e.g. “name of your dog”), since the attacker could be able to discover this information using public available data or social networks.

Several studies have shown that guessing (inappropriate) passwords is a very effective attack, so we cannot stress enough the importance of using appropriate passwords. The passwords should therefore be long enough, include upper- and lower-case letters, numbers and symbols, not use sequences, not include any association with the user and passwords should not be recycled.

Analyses of stolen passwords that subsequently circulated on the web showed that the most common passwords (globally) were password1, abc123, password, qwerty1, fuckyou, 123abc, iloveyou1, etc. Research has also shown that 1000 roots of certain words (e.g. “letmein”, “temp”) in combination with 100 add-ons (“1”, “abc”, etc.) recovers about 24% of all passwords, and by taking into account personal data, dates of birth, etc., it is possible to guess as many as two thirds of all passwords within a month (Schneier, 2008).

While it is true that password formatting patterns change over time, the following shows typical password formatting mistakes and of course, not changing your password is also a common mistake. A password that we suspect has been misused should be changed **immediately**.

Changing passwords

All systems that use passwords to authenticate users should also be able to change passwords. It is essential to change a password whenever we suspect that it has been disclosed to unauthorised parties or stolen.

Some organisations also have a security policy that requires users to change their password periodically (every certain number of days). However, such policies are being abandoned. If users are forced to change their passwords too often, users start choosing easy-to-remember passwords, or they start writing down their passwords, e.g. on a sheet of paper. This reduces security, so it's not surprising that a few years ago, both security experts and technology giants such as Microsoft started advising against enforcing policies of changing passwords periodically.

Password management systems

The first step to better security is to design passwords properly. Once we have well-designed passwords, we are faced with the problem of how to store them in such a way that they are not forgotten, or that an attacker is unable to get to them because of improper storage. Fortunately, the problem can be solved with some self-discipline and the use of password managers – special applications that serve as a repository for all our passwords, digital certificates and encryption keys. Such applications allow passwords to be entered in a special encrypted file, and can also attach files (e.g. digital certificate files or other encryption keys) in this protected storage. This file serves as a repository for passwords and is protected by a single password.

Today, there are many password managers available on the internet,[32] many of them free and open source. As mentioned above, passwords are one of the most important protection mechanisms, so they must be appropriate and their storage must be secure. Following the rules for creating appropriate or sufficiently secure passwords is therefore the first step in improving the security of our information and information systems. Safe and secure password storage makes it easy to use long and complex passwords and protects us from losing or forgetting passwords that we use less often. In addition, some password management systems help prevent attacks by logging keystrokes – keylogging, as they allow you to fill in the password fields automatically, thus disabling keylogging via keystrokes on the keyboard.

Adequate backups of your password stores should also be ensured. You may also warrant consideration of uploading the password to a private cloud, but in this case 2FA or MFA should be used for securing cloud access, since cloud systems are internet facing systems, with high exposure. Of course, it goes without saying that you must ensure that the password for accessing your password storage should not be lost.

Advanced authentication systems

The most common way to identify and authenticate a user today is through a combination of username and password. However, passwords have their limitations.

Recently, alternative authentication methods have become increasingly popular. There are other ways to authenticate that do not require passwords. One option is to use smart cards or hardware tokens containing a microprocessor and appropriate

[32] Keepass, Lastpass, Bitwarden, Lesspass, etc.

cryptographic mechanisms to authenticate or deny access to data. This method requires additional hardware and software (card reader, USB token[33], etc.)

Another option is to use one-time passwords. In this case, for example, logging into the system requires entering a new password each time. One-time passwords are created by one-time password generators, which can be hardware (a special device with a screen that displays a one-time password) or software (e.g. running on the user's mobile phone). One-time password generators are often used in combination with two-factor authentication (2FA) or multi-factor authentication (MFA). Two-factor authentication refers to authenticating a user by combining two independent components (factors). A typical example is a bank card, which requires a PIN number or the use of two passwords, one of which is a one-time password. The user will first have to enter their username and password (first factor), and then the login service will send an additional one-time password to their mobile phone (second factor), which they will then use to successfully log into the system. Two-factor authentication or two-step login thus provides an additional layer of protection and significantly reduces the risk of intrusion. It is therefore recommended to enable two-factor authentication in all services that allow this type of login.

Shared secrets

As mentioned earlier, most systems, especially business systems, use one of the password recovery schemes. These systems are used in case the user forgets the password, but they

[33] USB tokens are USB devices that work like smart cards. They are offering password management, encryption, two-factor authentication, and digital signing, but they do not need a special card reader device. Instead, they can be inserted in a universal serial bus (USB) connector.

also have their limitations. One of the main limitations is that these systems are prone to abuse (e.g. by a malicious system administrator).

A possible solution to ensure secure password storage or password recovery is called secret sharing or secret splitting. These are special methods of distributing encryption keys among multiple individuals, but these encryption keys are designed in such a way that multiple keys (but not all of them) must be used for access. So, we can create, for example, 10 different keys, and decryption may be possible with any three keys. These systems are also called threshold cryptographic systems, where encryption keys are distributed among several entities (persons), and at least a certain number of these persons must participate in the decryption.

Secret sharing systems are useful in many applications. These systems can ensure that parts of the keys are located in multiple locations, making it more difficult for an attacker to steal them. Another option is to share responsibility between several people who are not fully trusted. For example, only the bank manager can unlock the vault in a bank, but if he or she is not available, three staff members can unlock it together. Other systems are possible as well, e.g. one general can be replaced by ten soldiers (vault could be unlocked by one general or, if he is not available, by ten solders), etc. With the help of a cryptographic secret sharing system, it is possible to set up a system to keep our passwords and encryption keys safe in case of accident, death or unavailability of key users.

To conclude, passwords are most used security mechanism and should generally be complex and long enough to provide the desired level of security. Usually complexity and length provide more security, but those passwords less easy to remember. Access passwords can usually be reset or recovered and sometimes data or systems could be accessed directly by users with higher privileges, persons with so-called master key or with forensic tools, so it is important to be aware that password only does not guarantee the security of the data or the system. Regarding so-called “biometric passwords”, it is important to be aware that they cannot be revoked or changed. Biometrics should only be used for identification and not for authentication.

Another protective mechanism are encryption keys and we usually find them in the form of digital certificates or as special devices (hardware tokens). All these mechanisms could be complemented with two-factor authentication (2FA) or multi-factor authentication (MFA). For secure storage of passwords (and software encryption keys) the use of password management systems is recommended.

Physical security

Physical security is ensured by physical protection (alarm devices, video surveillance, etc.) and by controlling and recording physical access to the key parts of the information system. Physical security of portable electronic devices is also considered the most important measure to prevent data theft or misuse.

Additional measures, both appropriate software and certain hardware, can make unauthorised access to the system more difficult in the event of physical access. An important element in preventing unauthorised access to information is both the encryption of data media and the implementation of procedures for the permanent deletion from data media or the appropriate destruction of data media (e.g. commissioned destruction) Discarded computer components containing data carriers (e.g. hard drives, mobile phones, as well as internal data storage on different peripheral and IoT devices) may contain sensitive data that can be misused.

One of the attackers' techniques in the case of physical access is to install a keylogger, a device that can record or intercept the user's keystrokes (e.g. when they enter the password). Such devices are relatively inexpensive and attackers can build them themselves.[34] The attacker simply plugs the device between the keyboard and the computer, and the device then stores (and, if wireless, transmits) all the user's keystrokes on the keyboard. While older keyloggers could be detected visually, modern ones are so miniature that they can be hidden in a cable. There are also software keyloggers, which are special (malicious) applications that intercept keystrokes. These applications are also available for mobile phones. While it is possible to protect against hardware or software keystroke interception by using the on-screen keyboard, this protection works if the attacker is not recording the content of the display.

Similarly, we need to be careful when installing different applications, as some of them may have "dual function" – in addition to the basic function, they can also have hidden features to steal data, allow remote access, etc. It is a good idea to be careful when connecting unknown devices, such as "found" USB sticks or similar devices that may contain malicious code that can be planted on your computer when you connect the device.

The next more well-known attacking technique is the execution of an evil maid attack. An evil maid attack is an attack on an

[34] Some of the most known commercial devices with these abilities are *Rubber Ducky* (it is keyboard emulator) and *Bash Bunny* (keyboard, Flash drive, Ethernet adapter and a serial device emulator). However, there are several open hardware projects with detailed instructions how to build similar device for a couple of euros.

unattended device, in which an attacker with physical access alters it to get access to the device, or the data on it at a later time. Usually, this type of attack is used to physically access a computer with encrypted disks, booting the computer using a USB stick or CD and installing a software keystroke logger on the boot sector of the hard disk. In 2009, well-known information security expert Joanna Rutkowska demonstrated a practical evil maid attack on a computer fully encrypted with the well-known *TrueCrypt* encryption program. She developed a special program that slightly changes the original *TrueCrypt* program code, which asks the user for a password. The changed program code intercepts the typed password, stores it in a particular location on the disk and then passes it on to *TrueCrypt*. The special application can then be used to extract the stored password the next time the computer is physically accessed, thus bypassing encryption protection (Rutkowska, 2009).

According to some media reports, this is how the Israeli secret service obtained the access to the data on a computer of a Syrian diplomat who had left his computer unattended in a hotel room in London in 2006 (Gardham, 2011). The data obtained that way had proved that Syria was building the secret Al-Kibar nuclear facility in the desert (in IAEA documents it is also referred as Dair Alzour). The nuclear facility was subsequently bombed in Operation Orchard (also known as Operation Outside the Box) on 6 September 2007.

The evil maid attack can be defended against using smart cards or hardware tokens, which contain a microprocessor and a digital certificate that unlocks access to the data. Of course, in this case, we need to ensure that the smart card itself is properly physically secured. Protection (at least in part) may also be implemented using embedded (BIOS) hard disk encryption and the use of the TPM module (Trust Platform – this is a computer-integrated crypto-processor designed to secure the storage of encryption keys). A third option is to boot the computer from trusted removable media, but this is less useful in practice.

It is important to consider security of access to all output devices, especially printers and displays. Particular attention should be paid to network printers, where data transmission from the computer to the printer is generally not encrypted, and modern printers (especially larger multifunction devices) have built-in data storage on which documents in the printing queue are stored. This memory can be removed from retired (or stolen) printers, and the latest documents that were printed on this device can be reconstructed from the memory with relatively simple digital forensic analysis techniques. It should also be noted that modern printer servers are usually storing logs about the documents that have been printed (which user printed them, from which computer, the number of pages, the document title, etc.), but in some cases they also store the entire content of the documents that were sent to the printer for printing.

When using a laptop in public places (e.g. in a café, airport), physical security is even more difficult to ensure, as the content of our screen can be seen by all (random) passers-by. Polarising filters are an interesting solution to this problem, providing at least some protection from the prying eyes of people in the vicinity of your computer (or mobile phone) screen. These filters are sold as “privacy filters”, and when placed on the screen, they block the view of the screen from the side. If you look directly in front of the screen, the image is visible (although the light transmission is reduced by about 40%), but if you look at the screen from an angle, the content is invisible or at least heavily obscured.[35] As mobile phones are becoming more and more an important attack vector, buying polarising (privacy) filters for mobile phones should be considered.

[35] Recently some laptop manufacturers started to sell laptops with built-in polarisation filters. They are marketed as laptops with privacy screens.

There are some attacks that require the physical presence or proximity of a computer, but these are more difficult to implement in practice or require quite specialised equipment. One such attack is the Cold Boot attack, which can be used to reconstruct the contents of the working (temporary) RAM memory from a powered-off computer and gain access to encryption keys, for example. Another is the tempest attack which involves intercepting and reconstructing the electromagnetic signals (allowing, for example, the reconstruction of the display on a computer screen) emitted by computing devices into space.

It is important to remember that physical security must be provided to the network as well. If an organisation provides free Wi-Fi connections to its visitors or even complete strangers, it must ensure that users of such a Wi-Fi network cannot access the organisation's network where company computers or even servers are located. It is necessary to pay attention to multi-user environments, as users with lower privileges can use so-called escalation of privileges to gain unauthorised access to parts of the system that are otherwise inaccessible to them.

Tempest attack

Tempest (*Transient Electromagnetic Pulse Emanation Surveillance Technology* or *Transient Electromagnetic Pulse Emanation Standard*) is a method of intercepting temporary electromagnetic signals. While the method has been known since the middle of the last century, there is very little published research in the field. Tempest attacks are based on the fact that computer or electronic devices emit electromagnetic signals into the environment, and these signals can be intercepted and "reconstructed" in the vicinity of the attacked device. The first publicly published paper on tempest was by Dutch researcher Vim van Eck in 1985, hence the terms Van Eck Snooping or Van Eck Phreaking are also used for this eavesdropping technique. The term “tempest” is therefore sometimes used as a synonym for unwanted electromagnetic radiation that spreads in an uncontrolled manner and allows sensitive data to leak out. The protection against this type of interception of information is called emission security or EMSEC.

Most electronic equipment inadvertently emits electromagnetic interference (EMI)[36] emanations. The electromagnetic signals emitted by the monitor, keyboard, hard disk and other electronic components of a computer or other electronic device can be intercepted and reconstructed by special devices from a distance of a few dozen to a few hundred metres in such a way that an attacker can see the image on the monitor, which keys the user is pressing, what data is being written to the disk, etc. Data from EMI emanations can be also leaked through power lines.

This way the passwords or unencrypted data can be intercepted before they are encrypted in the computer. However, the eavesdropper does not need to have direct physical access to the device being eavesdropped on, as it is possible to carry out a tempest attack remotely, even up to 1 km away (under ideal conditions, practical attacks usually have a much narrow field from which they can occur, normally maximum a few meters) according to some studies. While a tempest attack requires quite specialised equipment, in recent years this equipment has become more widely available, so it is not surprising that security researchers were able to break the secrecy of Dutch voting machines in 2006 and Brazilian voting machines in 2009 (the machines that allowed the casting of an electronic ballot at the polling station) with a tempest attack.

Protection against tempest attacks on classified information in the field of national security is usually required by the legis-

[36] EMI – electromagnetic interference.

lation regarding the protection of classified information. This legislation requires that devices handling classified information marked as “CONFIDENTIAL” or higher must be protected against tempest attacks. There are also some international standards on tempest protection (so-called shielding standards), the most known are NATO[37] standards. Most of those standards are classified; however, some of their elements are publicly available.

There are some technical solutions for tempest protection, but not all of them are appropriate. Transmitting interfering signals is not useful in practice. The most used solutions include metal shielding. This creates a Faraday cage around the device to prevent electromagnetic signals from “leaking” into the surroundings. The protection must also include appropriate modifications to the device’s power supply, as electromagnetic signals may also leak into the surrounding area through power sources.

It is now possible to buy special tempest-certified computers on the market, which are properly shielded and made of specially designed electronic components that reduce tempest leakage. There are also solutions for shielding a whole building with metal (or to build so-called safe rooms) to prevent information leakage. These solutions are also available for the private sector and are quite affordable today.

Leakage of tempest radiation can be reduced by using shielded cables, which should be as short as possible, and by installing filters to reduce electromagnetic interference, also known as EMI filters.[38] However, there are also some programming solu-

[37] NATO – North Atlantic Treaty Organization is an intergovernmental military alliance between 27 European countries, 2 North American countries, and 1 Eurasian country (as the situation is in 2022).

[38] EMI filters, also called EMI suppression filters can be used to protect against the impacts of electromagnetic interference by suppressing electromagnetic noise transmitted through conduction and/or noise from grid power.

tions based on the use of specific tempest prevention fonts. These fonts are designed in such a way that the reconstructed image is blurred by the tempest attack. These techniques do not completely prevent a tempest attack, but they do raise the threshold of difficulty of carrying out such an attack.

Backup

The primary task of backup is to make copies of data that can be restored in the event of a hardware failure, hacker attack (e.g. by crypto-viruses), user error (e.g. deletion or overwriting of data) and other similar events. The loss of critical data may cause serious financial problems for an organisation. Operational interruptions lasting more than ten days may have permanent consequences for the organisation's operation. The problem is not only the permanent loss of data but also the damage caused by the interruption of work or the business process. Therefore, along with the implementation of backups, it is important to also have a disaster recovery plan in place.

Backups can be performed manually (on demand) or periodically. As it turns out, humans are not very consistent when it comes to manual backups. So it makes the most sense to automate the backup process. There are several backup strategies. The first is the full or mirrored backup, where each backup covers all the selected data.[39] The advantage of this approach is that the updating of data is faster, but, on the other hand, the creation of a single copy is more time and space consuming.

[39] Please note that solutions like RAID can provide enhanced data protection, however it should not be considered as a backup! (RAID – Redundant Array of Independent Disks is a data storage virtualisation technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.)

Such archived data can be either compacted (to save space) or encrypted (to protect data from unauthorised access).

The second strategy is incremental backup, where each backup includes only the data that has changed since the last backup. This strategy is less time and space consuming, but it is more time consuming to recover the data. Also, if one of the increments fails, the data cannot be restored correctly, as the first (full) copy of the data as well as all the differences (increments) are needed to restore the image. The longer the period between the full copy and the copy we would like to restore, the more incremental copies (so-called increments) are required.

The third strategy is differential backup. It operates by backing up the modified data between the full copy and the current state. In the case of restoring, we only need the last full copy and the latest copy (or the copy we want to restore). This type of archive is safer and faster than an incremental one but slightly more space consuming.

As outlined above, it makes sense to compress and consider encrypting the data in a backup archive. We could also use deduplication, the process of eliminating duplicates, which helps us to reduce the amount of storage space used. When implementing backup archiving, it is important to consider making backups not only of important data but of the entire system (including operating system and installed applications), so that in the event of a major failure, the system can be restored to its original state more quickly.

An important question is where to store the data. The most obvious option is to store it on an external data carrier (such as a portable drive, or a dedicated NAS device[40]), but to improve security, we should consider the creation of a backup copy to

[40] NAS – Network-Attached Storage is a file-level data storage server providing data access to clients over the computer network.

an external location, or better yet, on several external sites. One option is also to store backup data in a cloud; however, it is very important to understand that data in the cloud are not under your control and therefore consider using the encryption. Use of cloud computing entails a certain dependency on the service provider (which can even lead to a so-called “vendor lock-in”), and the availability of data in this case also depends on the availability of the cloud. This does not mean only possible cloud service failure, but also possible internet connection failure. So, the use of cloud services should be subject to serious consideration and maybe used for a secondary backup location because the cloud infrastructure could be prone to failure too.

In the case of emergency, it is important, that backups are quickly available. Usually this is achieved with local backup. But in case of a natural disaster event (fire, flood, quake, other) original data and their local backup could be damaged. In that case an external copy of the data could be a lifesaver. Therefore, it is a good strategy to implement the local backup (for instance in a NAS located within the organisation), and then archive it to an external location. Employees devices such as laptops that are often carried with them or used when working from home, can be backed up via a VPN[41] connection.

The so-called “Rule 3-2-1” describes what should the good backup strategy be. It explains as: there should be 3 copies of data, on 2 different media, with 1 copy being off site. The rule was later upgraded to the hard-core “3-2-1-1-0 rule”, which explains there should be 3 copies of data, on 2 different media, with 1 copy being off site, with 1 copy being offline, air-gapped or immutable and with 0 errors by regular verification (Vanover, 2021).

[41] VPN – Virtual Private Network.

Several solutions are available on the market today for the implementation of backups. Nevertheless, the creation of a good system for backups requires consideration and smart organisation. It makes sense to implement an automatic solution that allows storing multiple data versions. It also makes sense to store important data in multiple locations, and if data is stored externally (especially in the cloud), it should be protected with encryption. It is necessary to ensure that, in the event of an emergency, the data is available and can be quickly restored. Therefore, it is not enough simply to just implement a backup solution, but it is crucial that performance and reliability of backups is verified in practised regularly.

Encryption

Encryption is the process of encoding information (text messages, files, speech, video, etc.) into a form that cannot be understood by unauthorised persons. Cryptology is the science concerned with secure data communication and secure storage of data. It encompasses both cryptography, which is dealing with encryption and obscuring the content of data, and cryptanalysis, which is dealing with revealing of encrypted data. Cryptography can therefore be used to prevent communications from being eavesdropped on, while cryptanalysis is concerned with breaking encrypted messages.

In encryption, content (sometimes called plain text) is converted by an algorithm and a password (key or passphrase) into a form that is difficult or impossible to reconstruct back to its original form without the password (sometimes called cipher text). Strong encryption is therefore the most effective way to protect the content of messages, files, etc., from unauthorised access. In addition to enabling privacy, modern cryptography protects our financial transactions, secures our data on storage media and in the cloud. It can be used to provide digital signatures and integrity checks on data and software. In some cases, we are also legally obliged to protect certain categories of sensitive data with encryption.

Alongside cryptography, we should briefly mention steganography. It is a set of methods for hiding messages that enables us to share messages that are hidden in plain sight, by being disguised inside other files or regular messages. They implement the so-called invisible encryption, electronic watermarking and marking files with electronic serial numbers. Steganography methods can be used in both the physical[42] and digital environment. In combination with cryptography, steganography enables the implementation of plausible deniability – plausibly deniable encryption. Typically, this is used for concealing encrypted data into other encrypted data. From user perspective works the following way. The user has two encrypted keys: one unlocks the basic encrypted data, while the other unlocks the hidden encrypted data. This is particularly useful if the user is forced to disclose their encryption keys – in this case, they disclose only the first key, thereby not giving access to the hidden data. Plausible deniability and steganography systems are therefore especially useful for those living in non-democratic countries.

It should be noted that cryptography is not all-powerful. Cryptographic implementations can be attacked through weaknesses in cryptographic algorithms or weaknesses in the implementation of these algorithms. More frequent are attacks on cryptographic keys and passwords and indirect attacks on

[42] For instance, some laser printers print a sample of small yellow dots on each printed paper sheet, the layout of which contains information about the printer serial number and the date and time the document was printed.

cryptography (channel side attacks). However, security problems often arise because individuals do not use the cryptography in the proper way. The security of a cryptographic implementation depends, in a narrower sense, on the cryptographic algorithm used, and the length of the encryption key or the password adequacy used for encryption. In general, using encryption keys is better for security, because the key could be longer and have higher entropy when compared to passwords. But using passphrase is usually much easier. We can also use a special hardware – a smart card – which can be used to easily unlock encrypted data.

Since access to encrypted data depends on a password (or a smart cards), we need to make sure not to lose them. So, when using encryption, it is essential to introduce appropriate mechanisms for revoking lost passwords and to securely restore access to the data user loses their password or a smart card.

Transport-level encryption and end-to-end encryption

Regarding the implementation of encryption of the communications, two concepts apply. One is to use encryption at the data transfer level where the message is encrypted only during transfers between different servers (but not on the servers). In this case data at the target server is decrypted and then stored on a server or forwarded to another server (in that case it could be re-encrypted, but with different key). The second concept is encrypting the entire communication path. This concept is also known as end-to-end encryption (E2E). Here, an encrypted session is established between each endpoint (e.g. two communication terminals), which means that communications are encrypted along the entire communication path from user A to user B. Therefore, they cannot be eavesdropped by the network infrastructure provider or by the communications service provider (however, it could be intercepted at the source or target endpoint).

Using the example of email, the use of transport-level encryption involves the email client establishing an encrypted communication session to the mail server over which outgoing email is transferred. However, this mail is stored on the server in an unencrypted format. If the email needs to be forwarded towards other servers, this server then establishes a new encrypted session to the next server through which it forwards the email. And so on, to the destination server. In this case, the electronic message is encrypted during the transfer, but an attacker who has access to one of the interface servers will be able to read the message (including traffic data).

Using end-to-end encryption, the email example would mean that user A's message would be encrypted for user B. The message is encrypted the entire time it is transmitted from one user to another and is also stored in encrypted form on all intermediate servers. The message can be decrypted and its contents viewed exclusively by the final recipient. In this case, eavesdropping on the intermediate infrastructure is not possible, but the intermediate servers can record traffic data – who is communicating with whom, when and to what extent.

Man-in-the-middle attack

One of the more common attacks on encryption is the man-in-the-middle attack (MITM), where the attacker impersonates both communication partners to intercept their encrypted communications. MITM attack can also be carried out between the client and the server, e.g. web browser and web server.

In a man-in-the-middle attack, the attacker first places himself between the two communication partners (e.g. between the client and the server), where he intercepts the communication between them. He then starts to spoof both – presenting himself to the server as the client and to the client as the server. In this way, the client establishes an encrypted connection; not to the real server, but rather to the attacker's fake server. The server also establishes an encrypted connection; not to the real client, but to an attacker impersonating the client. At this intermediate point, the attacker decrypts the traffic and thus gains insight into the content of the otherwise encrypted communication.

A man-in-the-middle attack can be prevented by checking encryption keys or digital certificates, for which several techniques are available. On the web, this is done by digitally signing server certificates from trusted certificate authorities (CAs) or by setting up a so-called web of trust, but there are also other technical solutions, e.g. digital certificate pinning, Trust On First Use/Persistence Of Pseudonym (TOFU/POP), etc. Another such mechanism is HTTP Strict Transport Security (HSTS), that allows web servers to require that web browsers should interact with them using only HTTPS connections (this helps to protect websites against MITM attacks such as protocol downgrade attacks and session hijacking). Modern browsers are designed in such a way that they try to detect several MITM attacks and they warn users of potential risks regarding expired, self-signed or improper certificates.

There are several techniques for performing MITM attacks, for instance *IP*[43] *spoofing attack*, when an adversary masks

[43] IP – Internet Protocol, IP address is a unique address that identifies a device on the internet or a local network. IP addresses serve two functions: network interface identification and location addressing.

their identity by presenting themselves with the IP address of a legitimate device, *BGP*[44] *hijacking*[45] when attacker maliciously reroute internet traffic by falsely announcing ownership of groups of IP addresses, called IP prefixes, *DNS spoofing* (also called *DNS poisoning*), where adversary intercepts DNS request and returns the address that leads to its own server instead of the real one, *HTTPS*[46] *spoofing* (also known as *homograph attacks*), where attacker registers a domain name that is similar to the target website (and also SSL[47] certificate to make everything look more legitimate). This attack exploits a Punycode standard that enables the registration of hostnames that contain non-ASCII characters. Other techniques for performing MITM attacks include *Man in the Browser (MITB)*, where an attacker is compromising a web browser used by the user to perform eavesdropping, changing the displayed content, perform data theft, etc. By *SSL stripping*, an attacker downgrades the communications between the client and server into unencrypted format and then intercept (and possibly modify) communi-

[44] BGP – Border Gateway Protocol, is the routing protocol of the internet that provides directions so that traffic travels from one IP address to another as efficiently as possible. While DNS servers provide the IP addresses, BGP provides the most efficient way to reach that IP addresses.

[45] By BGP hijacking, internet traffic can go the wrong way in order to be monitored or intercepted, 'black holed', or directed to fake websites. In these cases fake websites can present legitimate HTTPS certificates. Example of this is an attack on South Korean cryptocurrency platform KLAYswap in February 2022, where attackers used a Border Gateway Protocol hack in to steal around 1.9m USD (Nair, 2022).

[46] HTTPS – Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol, which is the primary protocol used to transmit data between a web browser and a website. HTTPS is encrypted, which increases security of data transfer over the internet.

[47] SSL – Secure Sockets Layer is a cryptographic protocol designed to provide communications security over a computer network. It is deprecated from 2015 by TLS – Transport Layer Security, which is also a cryptographic protocol designed to provide cryptography, confidentiality (privacy), integrity, and authenticity using digital certificates, between two or more communicating computer applications.

cation. Attackers can also use *session hijacking* (sometimes called *browser cookies theft*), where an attacker steals the user's session token (cookie) and uses it to access the user's account. There is also a special type of MITM attack where an attacker hijacks or spoofs email to perform further attacks.

This all means that just using encryption does not guarantee the adequate level of security. Encryption should be used the correct way and user should have some basic understanding of security to avoid potential risks.

Encryption of email and internet communications

We often exchange confidential information via email. Since technically email is more like a postcard than a sealed envelope, encrypting email messages would make perfect sense. However, for historical and partly technical reasons, encryption of communications has not taken hold in the field of email. There are two main protocols used for encrypting email, OpenPGP and S/MIME (Secure/Multipurpose Internet Mail Extensions), which, in addition to encryption, also provide sender authentication and digital signing of messages and allow end-to-end encryption. Unfortunately, they are quite rarely used in practice.

Alternatively in the world of email, transmission level encryption is now much more widely implemented. This includes mail clients connecting to mail servers using an encrypted connection, even though the exchanged email messages itself are not encrypted. It is therefore, recommended to check with your email service provider whether it supports and enables encrypted protocols. If your organisation has its own email server, it is best to enable only encrypted connections (and completely disable unencrypted connections) to the server.

It is also reasonable to implement a security protocol for the verification of the authenticity of email (SPF – Sender Policy Framework, DKIM – DomainKeys Identified Mail, and DMARC – Domain-based Message Authentication, Reporting & Conformance). These protocols make it much harder to send spoofed or phishing emails and thus to implement so-called director's fraud. The latter involves attackers sending a fake email to the company's secretarial or accounting email address from the CEO,[48] instructing them to transfer money to a specific transaction account. This is termed spear-phishing, where the attacker carefully examines his target and then uses this information to assume the identity of a person important to the organisation (CEO, supplier, etc.) and then executes the attack.

If an organisation owns or manages its own email server,[49] it is a good idea to install antivirus and anti-spam filters. It is also good to consider implementation of disk encryption on a server to protect the emails in the event of physical theft or physical access to the email server. However, encryption has gained significant traction in online communications in recent years, especially with the emergence of Let's Encrypt, a non-profit certificate authority that provides X.509 certificates free of charge.

More and more websites are available exclusively over HTTPS connections (modern browsers are also pushing the use of encrypted HTTPS connections over non-encrypted HTTP connections), and the use of encryption is also increasing by using other communication protocols. It is advisable to enable support for HTTPS connections for all websites, or even better, mandatory use of it. Organisations that use HTTPS on

[48] CEO – Chief Executive Officer or managing director.

[49] It should also be noted that biggest email providers are marking email messages as spam, if it is coming from mail servers which do not have the proper implementation of SPF, DKIM and DMARC security protocols and PTR records. DNS PTR record is used for reverse DNS lookups. It matches domain names with IP addresses and is therefore a security tool that mainly helps to check if the server's name is associated with the IP address from where the connection was initiated.

their websites (even if website does not contain any sensitive information) are outwardly showing that they care about security. In addition, modern web browsers are marking web sites without HTTPS as insecure, and the use of HTTPS also affects the ranking of a website on search engines, which means that it ultimately affects the visibility of a company online.

The concept of end-to-end (E2E) encryption is gaining ground also in interpersonal communication, especially in instant messaging and voice and video communication over the internet. The main push for adoption of E2E encryption on popular messenger platforms has come from the Open Whisper Systems, a software development group that started the development of Signal Protocol (their founders are now working under non-profit Signal Technology Foundation). Signal Protocol is a non-federated cryptographic protocol that can be used to provide end-to-end encryption for voice calls and instant messaging conversations and has been partially implemented or has influenced the encryption protocols used in other popular chat platforms, such as WhatsApp, Facebook Messengers, Skype, and Viber. Currently a major development in the implementation of end-to-end encryption is being held in group communication.

Encryption of mobile communications

The emergence of smart mobile phones has made strong encryption of instant messages, voice and video communications easily accessible to a wide range of ordinary mobile users. With the help of Android and iOS apps, we can keep our mobile communications well protected from interception.[50]

[50] There are several applications for secure communications but regarding the security model, used cryptography, implementation and operating, Signal application could be recommended (Signal is also open source and free).

The first devices for encrypting voice communications were developed during World War II. They were hard to use and the devices were colossal. First such a device, called *SIGSALY* used by United States military to encrypt voice communications, weighed 55 tonnes, and filled a medium-sized room (Boone, Peterson and United States, 2000). Today, we can see how quickly technology is evolving, since we can have a much more powerful devices for encrypting voice communications literally in our pockets.

In addition to appropriate encryption protocols for secure exchange and authentication of encryption keys, it is important that such applications also use appropriate codecs for audio compression. Choosing inappropriate codecs can present a security risk, as it can enable eavesdropping even if encrypted data transmissions are used. Researchers has shown that when using encryption with voice streams compressed using variable bit rate (VBR) codecs, the length of the compressed data packets depend on the characteristics of the speech signal. In other words, different sounds are encoded differently, and these small variations in packet sizes can be observed, and that could be used to reconstruct ("decrypt") encrypted data (researchers have shown that the lengths of encrypted VoIP[51] packets can be used to identify the pre-recorded phrases spoken within a call). Additionally, applications for encrypting mobile communications need to solve a number of technical problems (e.g. network latency problems, echo cancellation). In all this, however, these applications must also ensure the best possible user experience without compromising security.

It is therefore fundamental to understand that securing mobile communications is a complex process, among the many apps

[51] VoIP – Voice over Internet Protocol, also called IP telephony, is a group of technologies for the implementation of voice communications and multimedia sessions over Internet Protocol networks.

that advertise themselves as impenetrable, it is important to choose one that does more than just provide security on paper. Typical example is carrier voice encryption in mobile networks, which is usually done through A5/3 algorithm, which is generally considered safe. However, encryption in mobile networks could be degraded to older and already cracked A5/1 algorithm (or in some cases completely switched off) and most importantly – data are encrypted between mobile device and mobile station only, so an attacker can perform eavesdropping at the base station or at any later point in the mobile network. This clearly shows us that mere implementation of encryption does not automatically offer us protection against eavesdropping, we must understand how the encryption is implemented and what the limitations of security of the system are.

When selecting security solutions, it is therefore a good idea to consult the relevant experts rather than simply trusting the vendors of the solutions they offer.

Encryption of data media

To protect the data on your computer from unauthorised misuse or access, it needs to be encrypted, which is particularly important in case of loss or theft of mobile devices or external storage devices. With today's technology, it is very easy to encrypt data media (disks, thumb drives, etc.), and it is also very easy to encrypt an entire operating system or computer. Encryption options are already embedded in all modern operating systems. For example, BitLocker can be used in a Windows environment, *LUKS* in a Linux environment and *FileVault* in a Mac environment. Also, internal storage encryption is enabled by default on most modern mobile phones, some of them even do not have an option to disable internal storage encryption, which is a very good from the privacy standpoint.

There is no doubt that safe PIN or passphrase storage is important, and the same is true for recovery key that most of these systems usually offer. As the use of encryption can lead to data loss in the event of a data carrier failure or malfunction, it is essential to ensure that adequate backup strategy is implemented. The importance of backup when using data encryption cannot be stressed enough.

Wiping data

As outlined above, physical access to data media is one of the major risks of unauthorised access to data. The best solution is to encrypt the entire data carrier, but if this is not possible, the data that we no longer need should be overwritten or wiped. The process is also called file or data shredding; it is a process of irreversible file destruction, so that its contents could not be recovered.

Normally, the deletion of data does not, in fact, erase them permanently. In principle, deleted files (including those removed from the so-called *Recycle Bin* or *Trash* – a place where deleted files are temporarily stored unless they are permanently deleted), can be recovered by digital forensics techniques. If a file is to be deleted permanently, its contents must be overwritten with other data. That is not always an easy and reliable task. In certain circumstances, the content of overwritten files can also be (at least partially) restored by forensic analysis.

Several options or methods can be used for overwriting data intended to be permanently deleted. The simplest method is to overwrite the data with zeros only once. A slightly better method is to overwrite with random or pseudorandom data, preferably multiple times. There is also the option of deleting using a low-level format, but this method is not reliable.

If a hard drive contains sensitive data, it is best to use multiple overwriting passes using special methods where the overwriting is done in a specific pattern. The best known is the *Gutmann method*, which requires 35 overwrite passes following a specific pattern, but there are others as well. Therefore, when selecting software applications for overwriting or wiping data, it is a good idea to find out what erasing methods are supported by the application and choose one that follows established standards.

When overwriting data, we can choose to overwrite the content of files, overwrite the free space (space that is not occupied by the file system but contains the remains of deleted files), overwrite slack space (space that the filesystem occupies on disk but is not used; slack space is particularly problematic in the FAT file system[52]), overwrite the contents of the swap space (space that holds data that used to be in RAM and may include passwords and encryption keys) or overwrite the contents of the entire storage medium. The best option is the latter, if feasible.

It is important to remember that permanent deletion of only the content of files in journal file systems is not easy and above all not reliable. Permanent deletion of data on network file systems or in the cloud is even more unreliable. Deleting the contents of files is also unreliable if disk defragmentation has been used before deleting. In all these cases, the data are not located in one place on the data medium but (possibly) in several places. Some file systems even have implemented so-called snapshot technology and they can keep several previous versions of files.

Modern disks also contain certain reserved sectors where data may be stored (namely Host Protected Area (HPA) and Device

[52] FAT – File Allocation Table is a file system developed for personal computers in 1977, however later was adapted and extended and it is still used nowadays.

Configuration Overlay (DCO), which are used for hiding sectors of a hard disk from being accessible by the end user). Specific approaches are therefore needed to delete data in these spaces.

When we talk about wiping data, we should not have in mind only computer disks. Sometimes data on mobile phones,[53] SD cards[54] or other media should also be wiped.[55]

In view of the above, the best way to protect data is through encryption. If this is not possible, it may be a good idea to use one of the wiping methods to erase the data on the device you are planning to sell or dispose of. In addition, it is necessary to emphasise that devices containing data are not only computer hard drives but also various peripherals (e.g. printers). Many of these devices have built-in features that allow permanent deletion of all data in the internal data storage. For business organisations, it makes sense for their IT system administrators to check how data on these devices can be deleted and to perform such deletions periodically or at least when the device goes out of service or out of use. So-called end-of-life (EOL) devices could also be physically destroyed, which is usually done in specialised facilities.

VPN networks

Many organisations, especially those that are moving towards more home working, want their business information system to be accessible to remote users (e.g. for employees working from home or on business trips). This can include the use of

[53] Data on a mobile phone after factory reset could be recovered. For completely wiping the data from your mobile phone check for data erasing options or protect data with encryption.

[54] SD card – Secure Digital non-volatile memory card.

[55] Data on non-erasable media such as CD, DVD and other could be destroyed by physically destroying the media, for instance by shredding.

Virtual Private Networking (VPN) technology, which allows us to connect different networks or computers securely using (usually encrypted) tunnels. Through such a tunnel, users can access a remote network or remote servers in a similar way to being physically present on the corporate network or even redirect all internet traffic from a remote computer to the organisation's network through the tunnel. VPNs are also used to circumvent regional access restrictions (e.g. video or other content that is not available in one region, but can be accessed via a VPN connection from the other region) to avoid censorship and to connect securely to the internet via unsecured network connections (e.g. wireless networks). In the latter case, VPN server acts as a secure gateway to the internet.

There are several types of VPNs. Some are simply used to connect remote computers to an internal network, while others can connect entire networks to each other. Some VPN connections allow networks to be connected at the data link layer (this is known as the 2nd layer of the OSI model[56]) and some at the network layer (3rd layer of the OSI model). Through VPN connections, the organisation can provide its employees an access to the internal IT system or internal services of the organisation – e.g. application servers, NAS servers, printers. In short, through VPN remote authorised users can gain access to all those services that are not accessible outside the organisation. There are several different VPN solutions available today. When implementing, it is necessary to pay attention to security as well as throughput (the volume of traffic that can pass through a VPN). We also should not forget about ease of use for both users and maintainers. Certain VPN solutions have complex configuration, and this can lead to mistakes by IT support personnel.

[56] OSI model – the Open Systems Interconnection model is a conceptual model that characterises and standardises the communication functions of a telecommunication or computing systems.

The fact that VPNs are blocked on some networks can also be a problem. While this usually does not apply to public communications networks used by employees at home, restrictions can be encountered in hotels, cybercafés and abroad (especially in non-democratic countries). It therefore makes sense to consider using remote access solutions that are more difficult to block at network level or to use a solution that allows so-called obfuscation (hiding) of VPN connections.[57]

For remote access, it is of course important to protect access to the core network as well as to implement network segmentation within the organisation. This could be accomplished with a firewall, which can be used to set up general network access rules as well as specific rules for access to individual parts of the network. Sometimes it makes sense to use an intrusion prevention system that protects computer network from brute-force attacks by dynamically adjusting firewall rules according to multiple failed connection attempts or network traffic analysis.

It is important to mention that transparency and trust are vital in the VPN industry. While the technology is important, it is of the utmost significance to know how well the VPN infrastructure is protected, and is it maintained regularly?

While several VPN solutions for so-called "safe browsing" are advertised on the internet and through social media, we should be

[57] These methods of network traffic obfuscation are based on masking the network traffic in some other protocol, for instance HTTP or HTTPS, DNS (DNS tunnelling), ICMP (Internet Control Message Protocol, so-called ICMP tunnelling), etc. Normal network traffic is then encoded in other protocol (for instance HTTP request and responses, DNS queries and responses, etc.) so it is harder to block. The Tor project (https://www.torproject.org/) is developing so-called Pluggable Transports, which is a set of network traffic obfuscating techniques, used to circumvent censorship.

aware that these solutions are generally not suitable for organisations, especially if organisation wants to connect their endpoints (computers and other devices) through the VPN. In that case self-hosting solutions should be considered as best option.

But if we are talking about commercial VPN providers which are usually offering solutions for browsing on the internet through their gateways, several important should be raised. For instance, who is the operator of exit points (VPN gateways to the internet) and how is the user's data handled there? Are VPN connections really encrypted? Where are VPN servers and exit points located (in which country, under which legislation)? And, how trustworthy is the internet service provider of a VPN provider?

In 2016 Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO) with researchers from the University of South Wales and UC Berkley did research of the VPN applications for Android mobile phones. They tested 283 VPN applications from *Google Play Store* and found that 18 per cent of the applications failed to encrypt users' traffic, 38 per cent of the applications injected malware or *malvertising*, over 82 per cent of applications requested access to sensitive data such as user accounts and text messages, three quarters of the applications used third-party user tracking libraries and the majority of them had several security issues (for instance did not prevent DNS leaking,[58] etc.) (Ikram, Vallina-Rodriguez, Seneviratne, Kaafar and Paxson, 2016).

Also, a study from 2021 analysing different VPN products has shown that a lot of these products were owned or operated by the same company (for at least of 104 VPN products researchers found out that they are owned or operated by only 24

[58] DNS leaking refers to a security flaw that allows DNS requests to be revealed to DNS servers of the internet service provider, despite the use of a VPN service to attempt to conceal them.

companies) and that VPN service providers were not transparent with users regarding their owners and parent companies' locations. Research has also shown that VPN services were in different "privacy unfriendly" countries including China[59] and Hong Kong (up to 30% of VPNs had connections with or were owned by Chinese companies), but also Pakistan,[60] United Arab Emirates, United States of America,[61] United Kingdom,[62] Switzerland,[63] etc. (Youngren, 2021).

[59] China has a high level of surveillance and cyber spying (especially on foreign officials). It imposes obligations on companies, who are broadly required to help decrypt information (source: World map of encryption laws and policies). Also, VPN applications are generally not available on the Chinese Android and iOS application stores, and China is also known for blocking VPN connections from China to outside world.

[60] Pakistan law enforcement officers have various powers relating to decryption including requiring officers access to data, device or information system "in unencrypted or decrypted intelligible format" for the purposes of investigating the offence. Licensed mobile and telephony service providers must establish systems for monitoring telecommunication traffic and these systems must ensure that voice and data signalling information is uncompressed, unencrypted, and not formatted in a manner which the installed monitoring system is unable to decipher (source: World map of encryption laws and policies).

[61] United States of America is the founding member of the Five Eyes alliance, a major surveillance state. Its National Security Agency (NSA) invests heavily in backdooring encryption technology, and Federal Bureau of Investigation (FBI) can access almost any data by secret subpoenas (so-called National Security Letters).

[62] United Kingdom is a founding member of the Five Eyes alliance and has surveillance legislation (Investigatory Powers Act, or Snooper's Charter, introduced in 2016) that gives law enforcement strong surveillance powers.

[63] Switzerland is advertised as a safe haven for digital privacy, but in fact has one of the strictest anti-terrorism laws in Europe (Ibrahim, 2021). Also, Swiss Federal Act on the Surveillance of Post and Telecommunications and Federal Intelligence Service Act had introduced broad surveillance of all electronic communication (Schönenberger, 2016) (Schönenberger, 2018). Regarding intelligence cooperation, Switzerland has several bilateral agreements with EU and is bound by a Mutual Legal Assistance Treaty with the United States. It is also important to point out that at least two Swiss companies, CryptoAG (Miller, 2020) and Omnisec (Endres, 2020), were closely cooperating with foreign intelligence services and were selling rigged cryptography equipment.

It could be concluded that the trustworthiness of the VPN provider is of the utmost importance, therefore running a VPN on your own infrastructure and under your full control is worth considering.

Availability

An important part of information security is also the availability of information and systems. Availability ensures reliable and timely access to the information system when users need it. A reliable and available IT system in an organisation is the foundation for the smooth execution of work and business processes and therefore plays a key role in business efficiency. The failure or unplanned downtime of an IT system usually causes unexpected interruptions to business processes, resulting in unnecessary costs.

Organisations should therefore have a business continuity plan in place, which defines the measures to maintain a certain level of service in the event of hardware or software failure, but also evacuation procedures of equipment in case of natural or some other disaster. These are measures aimed at ensuring continuous operations or disaster recovery. At the hardware level, the measures mainly include the purchase and implementation of redundant computer, network and other hardware components, while at the software level it makes sense to implement all those solutions that protect information systems against attacks, user errors and software failures.

As the establishment of a business continuity system involves a certain financial investment, it is necessary to develop an appropriate plan to ensure that the organisation's critical functions are successfully established as quickly as possible and at the lowest possible cost. In this context, it is necessary to consider both the short-term and long-term consequences of an IT system failure for the organisation as a whole. However, we cannot stress enough the importance of regular testing of the business continuity plan, so you know if your organisation is prepared for a disaster.

Remote work

If an organisation wants to organise remote working even in the event of major crises or emergencies, it needs to design its information system to be available not only within the organisation but also for remote users.

A fundamental building block of the IT system's external accessibility is VPN technology, which allows employees to connect securely to the corporate network from remote locations. In this case, however, the security of the organisation's entire IT system must be designed in a significantly different way, as the security of the terminal equipment used by users accessing the organisation's internal network from remote locations must also be considered. Remote work is also causing extra stress on the VPN resources as well as to network security equipment (firewall, IDS/IPS), so organisations should be prepared for that, and have a plan for expand their capabilities.

If employees work from home, they must also have the appropriate technical equipment. In times of crisis, the latter may not be available (to buy), so it makes sense to keep them in stock. Alternatively, it is possible to make use of the BYOD concept (*"Bring Your Own Device"*). This is the practice of employees bringing their own personal devices (laptops, tablets, smartphones) to work environments to access business, personal and other data in the organisation's IT system or, when working from home, using their own personal devices to connect remotely to the organisation's IT system. While BYOD enables greater mobility and ease of use for users and in principle reduces hardware costs for the organisation, it also brings several risks, both in terms of business information security and the protection of personal data and information security in general. The risks include not only the increased possibility of losing devices (mobile phones and laptops), but also the issue of securing these devices according to the legal requirements regarding personal data protection, classified information, labour, and competition legislation. When using the BYOD concept and enabling remote working, it is therefore important that the organisation carries out a proper assessment of whether employees' private devices are sufficiently secure. Risks need to be identified, analysed and procedures and measures put in place to reduce or even eliminate these risks. At the same time, it is important to be aware that an organisation cannot impose overly strict security policies on employee-owned devices, as this could infringe too much on users' privacy or even motivate employees to take shortcuts. For the latter reason in particular, user education is also very important. Using different user accounts for work and private purposes is also a good strategy to reduce the risks.

It is important to anticipate that employees may need help when working from home, and that some maintenance work may need to be done on their computers (with their consent). It is therefore advisable to install appropriate software equipment on the computers to allow remote access in case such assistance is needed.

Video conferencing systems are becoming increasingly crucial for remote working, allowing companies to hold meetings between employees and business partners. Again, this requires the right equipment. For example, an external headset with a microphone will usually offer a significantly better user experience than a built-in microphone and speakers. It is also necessary to ensure that users working from home will have a sufficiently powerful internet connection, or that they will be able to use a mobile connection to access the internet. Some videoconferencing solutions also provide end-to-end encryption – even in the case of group communication – which is certainly important to consider when these systems are being used in business environments.

For companies, it is crucial that their information systems are designed in a way that enables the simplest transition to remote work if necessary. Business organisations should focus on building and maintaining the adequate infrastructure and ensuring that employees have the suitable skills and knowledge for remote work.

Anonymisation

At a times when we are confronted with the increasing collection and use of traffic data on the one hand, and with increasingly blatant attempts of censorship even in democratic countries on the other, many people are seeking technical measures that can be applied against that.

One possible type of protection against the collection of traffic data and restrictions on access to information on the internet, are anonymisation systems. These systems allow us to hide our real IP address while also allowing us to circumvent censorship restrictions. There are several types of anonymisation systems available. Most systems are intended for the anonymisation of online services, but there are also special applications aimed at the anonymisation of other services, e.g. P2P file sharing or other traffic.

It is important to realise that complete anonymisation is almost impossible in practice, because with enough motivation and, above all, a lot of resources, anonymisation systems can be subjected to a variety of attacks that allow an attacker to reveal the identity of their users. One of these techniques is *netflow* data analysis, which is performed to analyse traffic flow and traffic volume across the network. This can show which network node is communicating with another and can be used for tracking the users of anonymisation networks. But usually deanonymisation techniques require significant resources which means that they cannot be used on a wide scale. Using of anonymisation systems can consequently increase the level of anonymisation so the identity of the user of such a system is much more difficult to disclose.

Some of the first anonymisation systems were anonymous proxies, which were the interfaces between the user and the website or service being visited. While proxy servers are still in use today, they are no longer used for anonymisation but for monitoring and analysing traffic (to protect users from malicious code or unwanted content) or to speed up web browsing (by caching static web content).

The *Tor anonymisation and anti-censorship network* has set a standard for modern anonymisation systems. It is a distributed network of anonymisation servers, between which each user's encrypted traffic is routed until it leaves the network at one of its exit nodes. To use the *Tor network*, the user installs a *Tor client* or a special *Tor browser* on their computer, which redirects their web traffic to the *Tor network*. In addition to anonymisation, the *Tor network* also offers the possibility to publish online content anonymously or to offer various network services anonymously. The developers of the *Tor network* have also built in so-called hidden services. These are (mostly web and mail) servers that are located within the Tor network and are not accessible from the “regular” web. They are accessed using special URLs[64] with the extension .onion and they can be accessed only from the *Tor network* (hence the name dark web).

Unfortunately, due to human nature, anonymisation technology often attracts various illegal and undesirable activities. Alongside perfectly legitimate and legal content, the *dark web* is thus also home to a wide range of illegal content, from child pornography to marketplaces with stolen credit card numbers, illegal online betting sites and the like. Nevertheless, the use of the *dark web* is not illegal by itself. *Dark web* is not used only by hackers and criminals. It is also used by investigative journalists who want to communicate anonymously with their sources, *whistleblowers*, political dissidents and even intelligence officers. The *Tor network* is the only uncensored and unmonitored window to the world for many people in non-democratic countries. The network can also be used by all those who visit such countries as tourists or on business trips and want to avoid local censorship restrictions.

[64] URL – Uniform Resource Locator or web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

Conclusion

The provision of information security includes adequate infrastructure, protection of devices, data and applications and empowered users.

To ensure the overall information security of an organisation against cyber-attacks, it is necessary to implement security mechanisms at the level of the network, servers, user computers, peripheral devices and mobile devices (phones, tablets, etc.) Regular maintenance and updating of software and hardware equipment, at least basic physical security, implementation of a firewall or IDS/IPS system, a backup system and encryption should be provided in as many places as possible. This includes both the use of encrypted protocols wherever possible (for access to email and websites) and the implementation of data media encryption. It is recommended to use anti-virus and anti-spam software, applications to block online tracking technologies and so-called “junk” removers.

Users need to be made aware of the basic risks and how to protect themselves from threats. They should also be familiarised with how to choose appropriate passwords and, where possible, it is advisable to implement more advanced forms of authentication (use of one-time passwords, two-factor authentication, etc.)

Security policies should define procedures for protecting the organisation’s information, installing and updating software and hardware handling procedures, including the implementation of a data wiping policy. If remote access is required, a properly secured VPN network should be set up, and at least the basics of a business continuity system should be put in place.

It cannot be guaranteed that the above will provide total security. But with these measures, an organisation will increase its overall protection, improve the management of information risks and ensure that it has secure and reliable operations.

List of acronyms

BGP
Border Gateway Protocol, is the routing protocol of the internet that provides directions so that traffic travels from one IP address to another as efficiently as possible. While DNS servers provide the IP addresses, BGP provides the most efficient way to reach that IP addresses.

CD
Compact Disk, a digital optical disc data storage format.

CEO
Chief Executive Officer or managing director.

DDoS
Distributed denial-of-service attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming with a flood of internet traffic.

DNS
Domain Name System is the hierarchical and decentralised naming system that translates human readable domain names to machine readable IP addresses.

DVD
Digital Versatile Disc is a digital optical disc data storage format.

EMI
Electromagnetic interference.

FAT
File Allocation Table is a file system developed for personal computers in 1977, however later was adapted and extended and it is still used nowadays.

FBI
Federal Bureau of Investigation is the domestic intelligence and security service of the United States and its principal federal law enforcement agency.

Firewire
Also called IEEE 1394 or i.LINK is a high-speed computer data-transfer interface.

HTTPS Hypertext
Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol, which is the primary protocol used to transmit data between a web browser and a website. HTTPS is encrypted, which increases security of data transfer over the internet.

ICMP Internet Control Message Protocol
An error-reporting protocol that network devices use to generate error messages to the source IP address when network problems prevent delivery of IP packets.

ICT
Information and Communications Technology, is the infrastructure and components that enable modern computing.

IDS/IPS systems
Intrusion Detection/Prevention Systems; are solutions for the detection and/or prevention of network attacks.

IoT
Internet of Things, physical objects that are embedded with sensors and software, which connect and exchange data with other devices and systems over the communications networks.

IP
Internet Protocol, IP address is a unique address that identifies a device on the internet or a local network. IP addresses serve two functions: network interface identification and location addressing.

IT
Information Technology.

KGB (Komitet Gosudarstvennoy Bezopasnosti Committee for State Security)
KGB was the main security agency for the Soviet Union.

NAS
Network-Attached Storage is a file-level data storage server providing data access to clients over the computer network.

NATO
North Atlantic Treaty Organization is an intergovernmental military alliance between 27 European countries, 2 North American countries, and 1 Eurasian country (as the situation is in 2022).

NSA
National Security Agency is a national-level intelligence agency of the United States Department of Defence.

OSI model
The Open Systems Interconnection model is a conceptual model that characterises and standardises the communication functions of a telecommunication or computing systems.

OSINT
Open-Source Intelligence, a set of strategies and methods for the collection and analysis of data gathered from publicly available sources to produce actionable intelligence.

PTR
Pointer record. DNS PTR record is used for reverse DNS lookups. It matches domain names with IP addresses and is therefore a security tool that mainly helps to check if the server's name is associated with the IP address from where the connection was initiated.

RAM memory
Random-Access Memory is a form of computer memory that can be read and changed directly. Typically, is used to store working data and machine code.

RAID

Redundant Array of Independent Disks is a data storage virtualisation technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both. While RAID arrays can provide enhanced data protection, it should not be considered as a backup.

SD card

Secure Digital non-volatile memory card.

SSL

Secure Sockets Layer is a cryptographic protocol designed to provide communications security over a computer network. It is deprecated from 2015 by TLS – Transport Layer Security, which is also a cryptographic protocol designed to provide cryptography, confidentiality (privacy), integrity, and authenticity using digital certificates, between two or more communicating computer applications.

URL

Uniform Resource Locator or web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

USB

Universal Serial Bus.

VoIP

Voice over Internet Protocol, also called IP telephony, is a group of technologies for the implementation of voice communications and multimedia sessions over Internet Protocol networks.

VPN

Virtual Private Network.

WHOIS

A database which stores registered users or assignees of internet resources like domain name, IP address block or autonomous system data.

References

1. Boone, J. V. & Peterson, R. R. & United States. 2000. *The start of the digital revolution, SIGSALY secure digital voice communications in World War II*. Center for Cryptologic History, National Security Agency. Available at: https://media.defense.gov/2021/Jul/13/2002761542/-1/-1/0/SIGSALY.PDF.
2. Endres Fiona. 2020. Geheimdienstaffäre: Weitere Schweizer Firma rückt in den Fokus. SRF (Schweizer Radio und Fernsehen), 25. 11. 2020, https://www.srf.ch/news/schweiz/verschluesselungsgeraete-geheimdienstaffaere-weitere-schweizer-firma-rueckt-in-den-fokus.
3. ENISA. 2016. ENISA's Threat Taxonomy. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.
4. Gaillot, Vincent. 2001. How to use Google to find confidential informations. Posted on BUGTRAQ. Available at: https://marc.info/?l=bugtraq&m=100619108724992.
5. Gardham, Duncan. 2011. Mossad carries out daring London raid on Syrian official. The Daily Telegraph, 15 May 15th 2011. Available at: https://www.telegraph.co.uk/news/worldnews/middleeast/israel/8514919/Mossad-carries-out-daring-London-raid-on-Syrian-official.html.
6. Ibrahim Sara. 2021. Will Switzerland distance itself from the EU on mass surveillance? SWI, 8. 7. 2021, https://www.swissinfo.ch/eng/will-switzerland-distance-itself-from-the-eu-on-mass-surveillance-/46766024.
7. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. 2008. Lest

We Remember: Cold Boot Attacks on Encryption Keys. 17th USENIX Security Symposium. Available at: https://www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf.

8. Koch, Stephen. 2004. Double Lives: Stalin, Willi Munzenberg and the Seduction of the Intellectuals. New York: Enigma Books. ISBN-13: 978-1929631209.
9. Leyden, John. 2009. Russian spy agencies linked to Georgian cyber-attacks. The Register, March 23rd 2009. Available at: https://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/.
10. Long, J. and Skoudis, E. 2005. Google Hacking for Penetration Testers. Syngress, Rockland.
11. Markoff, John. 2008. Before the Gunfire, Cyberattacks. The New York Times, August 12th 2008. Available at: https://www.nytimes.com/2008/08/13/technology/13cyber.html.
12. Miller Greg. 2020. The intelligence coup of the century. The Washington Post, 11. 2. 2020. Available at: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.
13. Milmo, Dan. 2022. Russia unleashed data-wiper malware on Ukraine, say cyber experts. The Guardian, February 25th 2022. Available at: https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts.
14. Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar and Vern Paxson. 2016. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. Published in IMC ‘16: Proceedings of the 2016 Internet Measurement Conference, November 2016, p. 349 - 364. ISBN: 9781450345262, DOI: 10.1145/2987443.

15. Nair, Prajeet. 2022. Crypto Exchange KLAYswap Loses $1.9M After BGP Hijack. BankInfoSecurity, February 16th 2022. Available at: https://www.bankinfosecurity.com/crypto-exchange-klayswap-loses-19m-after-bgp-hijack-a-18518.
16. Newman, Lily Hay. A Year After the SolarWinds Hack, Supply Chain Threats Still Loom. Wired, Dec 8th 2021. Available at: https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/.
17. Nichols, Michelle. 2019. North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. Reuters, August 5th 2019. Available at: https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX.
18. Prince, Brian. 2009. Cyber-attacks on Georgia Show Need for International Cooperation, Report States. eWeek, August 18th 2009. Available at: https://www.eweek.com/security/cyber-attacks-on-georgia-show-need-for-international-cooperation-report-states/.
19. Rutkowska, Joanna. 2009. The Invisible Things Lab's blog: Evil Maid goes after TrueCrypt!. The Invisible Things Lab's blog. Available at: http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html.
20. Schneier, Bruce. 2008. Passwords Are Not Broken, but How We Choose them Sure Is. November 13th 2008. Available at: https://www.schneier.com/essays/archives/2008/11/passwords_are_not_br.html.
21. Schönenberger, Erik. 2016. Faktenblatt und Illustration zur «Kabelaufklärung». Digitale Gesellshcaft, 1. 9. 2016, https://www.digitale-gesellschaft.ch/2016/09/01/faktenblatt-und-illustration-zur-kabelaufklaerung/.

22. Schönenberger, Erik. 2018. Faktenblatt zur «Vorratsdatenspeicherung». Digitale Gesellshcaft, 27. 9. 2018, https://www.digitale-gesellschaft.ch/2018/09/27/faktenblatt-zur-vorratsdatenspeicherung-uebersichtlich-erklaert/.

23. Stoll, Cliff. 1990. The Cuckoo's Egg. New York: Pocket Books. ISBN-13: 978-0671726881.

24. Vancover, Rick. 2021. What is the 3-2-1 backup rule? Veeam blog, https://www.veeam.com/blog/321-backup-rule.html.

25. Voiskounsky, E. Alexander, Babveva D. Julia and Smyslova, V. Olga. 2000. Attitudes towards computer hacking in Russia. In Thomas, Douglas in Loader D. Brian, (ed.). 2000. Cybercrime, p. 56–84. London, New York: Routledge.

26. Zalewski, Michal. 2001. Against the System: Rise of the Robots. Phrack magazine, Volume 0x0b, Issue 0x39, Phile #0x0a of 0x12. Available at: http://phrack.org/issues/57/10.html.

27. Zetter, Kim. 2014. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Broadway Books. ISBN: 978-0-7704-3617-9, eBook ISBN: 978-0-7704-3618-6.

28. Youngren, Jan. 2021. Hidden VPN owners unveiled: 104 VPN products run by just 24 companies. https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/, April 19th, 2021.

29. World map of encryption laws and policies. Globar Partners Digital, https://www.gp-digital.org/world-map-of-encryption/.

9 789617 025248