Course Book

CYBER SECURITY AND DATA PROTECTION

DLMCSITSDP01

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

LEARNING OBJECTIVES

For companies working in information and communication technologies (ICT), the biggest challenge and top priority is protecting data and information. In **Cyber Security and Data Protection**, we will explain how to protect the most important assets in a company—you will learn which methodology, resources, and tools to use.

You will learn about the needs of companies, as well as how to develop a sound cyber security framework that protects digital information, data, and other equipment (ICT assets) in cyber space. Furthermore, you will gain insight into different cyber security models and learn how to determine which one is best for the situation at hand.

~~Today,~~ applied cryptography is a very important part of any IT system, as it results in one of the hardest building blocks in the cyber security domain. The reason for this is simple—the most important thing in any company ~~today~~ is the protection of data, information, and knowledge. They should be kept safe throughout their creation, use, transfer, and storage, which would be much more difficult without applied cryptography.

UNIT 1

FOUNDATIONS OF DATA PROTECTION AND IT SECURITY

STUDY GOALS

On completion of this unit, you will have learned …

- the basic terms of security and risk management.
- the basic terms and concepts of data protection and privacy.
- some examples of legal aspects of cyber security.

1. FOUNDATIONS OF DATA PROTECTION AND IT SECURITY

Introduction

Nearly every organization that exists today relies on data and information—they enable organizations to survive in the business space. The loss of this information has tremendous consequences and can lead to a business being forced to exit the market. Impairing the security of personal data does not only affect the organization, but also the individual to whom the data belong~~s~~. Therefore, protecting this information has become more and more important.

This unit will introduce a few basic concepts that will help you to understand security and data protection holistically. The explanations concerning legality will not only cover data protection and privacy, but also other legal aspects that play a role in cyber security. It is a field that is regulated more intensively over time and, in recent years, has seen an increased amount of legal regulation and discussion.

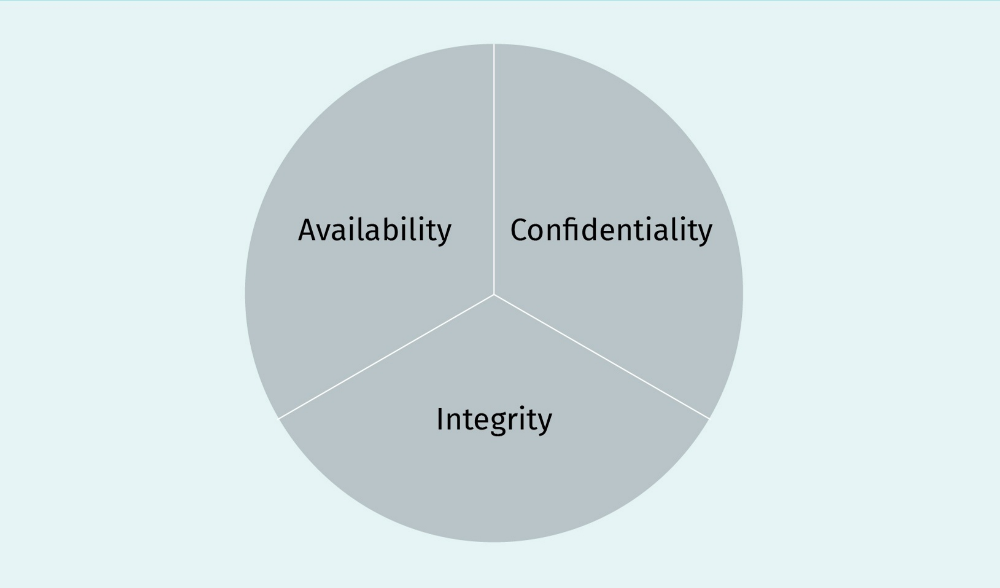
1.1 Terminology and Risk Management

During this course, the term "cyber security" is used frequently. Although "cyber security" and "information security" are frequently used as synonyms, they do not always mean the same thing. Some regulators require companies in the financial sector to have separate information security and cyber security functions. Where information security tries to secure information in its analogous form, cyber security tries to protect information that is vulnerable through the use of information and communication technology. In this course book, the term "cyber security" will also define the security of analogous information. When referring to standards and laws, the term "information security" will be used since it is commonly referred to within legal documents.

CIA triad
This model influences policies for information security within organizations.

The **CIA triad** of information security defines cyber security. Cyber security is put in place to protect the confidentiality, integrity, and availability of information.

Figure 1: CIA Triad of Cyber Security



Source: Created on behalf of IU (2020).

The “C” in “CIA” stands for confidentiality. It means that information is only made available to those authorized to have access. An attack on confidentiality could lead to the unintended disclosure of a customer database that is stored on a cloud storage space.

The “I” stands for integrity, meaning the maintenance and assurance of the accuracy and completeness of information over its entire life cycle. A hacker who, for example, changes marks in a university information system to increase a student’s grades, would impair integrity.

Finally, the “A” stands for availability. Information must be available when it is needed. Availability can be impaired when a system is attacked, for example, by a distributed denial of service (DDoS), rendering the system unavailable for use.

There are other security goals that are sometimes mentioned alongside the CIA. We can assign them to parts of the CIA, but they often stand on their own:

- “Resilience” ensures that systems are built with the ability to withstand an attack or outage.
- “Authenticity” ensures that personnel and users are who they say they are.
- “Nonrepudiation” means that a person cannot deny having taken action.

Information is protected by mitigation of risk; hence, cyber security is often seen as a part of risk management. This is achieved through a structured risk management process, consisting of

- identification of risk,
- analysis of risk,

- mitigation of risk, and
- reporting risks.

1.2 Core Concepts of IT Security

Cyber security consists of many disciplines and is often divided into different domains. Different organizations have developed frameworks specifically suited to their individual needs. The International Information System Security Certification Consortium, also known as (ISC)^2, classifies cyber security into eight different domains:

- security and risk management,
- asset security,
- security architecture and engineering,
- communication and network security,
- identity and access management (IAM),
- security assessment and testing,
- security operations, and
- software development security (International Information System Security Certification Consortium, n.d., How...? Section, para. 2).

The United States National Institute of Standards and Technology (NIST) considers the following aspects as part of cyber security in its standard family SP-800:

1. Information security governance
2. System development life cycle
3. Awareness and training
4. Capital planning and investment control
5. Interconnecting systems
6. Performance measures
7. Security planning
8. Information technology contingency planning
9. Risk management
10. Certification, accreditation, and security assessments
11. Security services and product acquisition
12. Incidence response
13. Configuration management (Bowen, 2008).

These lists show that a holistic cyber security program has a wide scope covering many aspects and domains—we will use a combination of both approaches to introduce a few of the core concepts of security.

The concept of “defense” works by assuming that one or more controls are broken, so other layers of defense must be able to protect assets. We cannot assume that border perimeters, such as the internal network, are impenetrable, or that resources inside that perimeter do not need to be protected. Instead, we assume that protection is also needed internally. Due to the new trend of resources outside the internal network (cloud computing, SaaS, etc.), it is crucial to consider all parts of the organization when implementing defensive measures.

Governance and Risk Management

Cyber security governance is used to proactively manage cyber security and implement and monitor necessary controls, but it must also align with the business in relation to the goals of the cyber security program. After considering the needs of the business, an organization develops its cyber security strategy and plan, and governance structures are then established. Cyber security governance boards, or risk committees, play a critical role as they decide on the way forward, which is influenced by whether the business, IT, and cyber security have the same priorities. A security policy and a plan to continuously improve and audit cyber security are developed, and then the governance aspect of cyber security oversees their implementation.

Risk management helps to identify, assess, and mitigate cyber security risks, as well as implement adequate controls in order to bring risks to a tolerable level.

Security Awareness

People play the most important role in securing the organization. Social engineering is an attack vector that manipulates people into performing actions that could harm an organization. Examples are phishing emails, unsolicited phone calls, or impersonation attacks. Security awareness helps to mitigate these attacks by making everyone in the organization aware of their duties and responsibilities concerning cyber security. An awareness program must be relevant for the audience, e.g., a user would receive different training to a security professional. Awareness, training, and certification are the components that make up the security awareness program. Finally, the success of the program should be monitored. An organization can monitor who completed their training or test the users' awareness by sending out fake phishing emails.

Identity and Access Management

Identity and access management ensures that users in an organization are identified and manages users' access to resources. A central concept that is employed is the Access Control List (ACL). An ACL includes the access rights for each resource. In the Unix operation systems such as Linux and BSD Unix, each user or group is categorized based on their authorization to either read, write, or execute rights for a particular resource. These categories are known as the rwx triple.

Identification and Authentication, Authorization, and Accountability is also known as IAAA and contains the following steps:

1. “Identification” means that a user states who they are. This can be achieved by typing in a username or stating one’s name at an entrance gate.
2. “Authentication” is the process where a user shows that they are the individual they claimed to be in step one. This should be done by presenting multiple factors, as one factor could be easily be compromised. There are five different factors:
   a) Something you know: Type 1 authentication (passwords, pass phrase, PIN, etc.)
   b) Something you have: Type 2 authentication (ID, passport, smart card, token, cookie on PC, etc.)
   c) Something you are: Type 3 authentication (biometrics such as a fingerprint, iris scan, facial geometry, etc.)
   d) Somewhere you are: Type 4 authentication (IP/MAC address)
   e) Something you do: Type 5 authentication (signature, pattern unlock)
3. “Authorization” checks which resources a user has access to. This is done via RBAC, DAC, or MAC and ACLs.
4. “Accountability” ensures that an audit trail, such as a log, exists. It traces the actions of users and records what they have done to prove their non-repudiation.

Network Security

Network security includes all means used to protect the CIA of the organization’s networks. There are many ways to protect a network, and here we will introduce some of them.

Encrypting the network traffic is a basic concept used to ensure that an attacker, if they have access to a network, cannot see information within that network. Nowadays, organizations should encrypt as much network traffic as possible in order to reduce the attack vectors by the maximum feasible amount. Non-encrypted protocols such as telnet or ftp must be avoided and replaced with their encrypted alternatives. When using wireless networks (WiFi), encryption is usually built into the protocols, for example, WiFi Protected Access 2 (WPA2).

A firewall monitors and controls incoming and outgoing traffic based on predefined rules. Originally, firewalls were placed at the outside perimeters of a network but nowadays, we also find them within organizations where they segment the network and ensure security in depth. Complex firewall structures are the new norm. Firewalls have developed over time in the following ways:

1. First generation firewalls, or packet filter firewalls, inspect each packet and filter it based on specific rules, usually on IP addresses and ports.
2. Second generation firewalls, or stateful filters, also maintain information based on the connection between two hosts.
3. Third generation firewalls, or application firewalls, understand certain applications and their vulnerabilities so that they can protect them.
4. Next generation firewalls (NGFW) can inspect connections on a deeper level. Intrusion Prevention Systems (IPS) learn from the behavior of hosts and network connections so that they can prevent attacks.

Software Development Security

The system development life cycle (SDLC) is the development, maintenance, and retirement of information systems. Security must be applied to all phases of the SDLC. The Open Web Application Security Project (OWASP) is a non-profit organization that publishes typical Web application vulnerabilities, but also develops standards on the topic of implementing software securely.

The OWASP top ten list, last updated in 2021, consists of the following ten vulnerabilities that are often seen in Web applications (Open Web Application Security Project, 2021):

- A1:2021—Broken Access Control: restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws so that they can have unauthorized functionality and/or data, such as access to other users' accounts and sensitive files, the ability to modify other users' data, or permission to change access rights.
- A2:2021—Cryptographic Failures: many web applications and APIs do not properly protect sensitive data such as financial, healthcare, and PII, applying cryptography either incorrectly or not at all. For example, they use algorithms and protocols that are weak or inadequate to the task, or weak keys. Attackers may steal or modify such weakly protected data to commit credit card fraud, identity theft, or other crimes. Without extra protection such as encryption at rest or in transit, sensitive data may be compromised and require special precautions when exchanged with the browser.
- A3:2021—Injection: injection flaws such as SQL, NoSQL, OS, and LDAP injection may occur when untrusted data is sent to an interpreter as part of a command or query, usually after passing on data from some user input field without verification. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- A4:2021—Insecure Design: even a perfect implementation of a web application will be insecure if it is not based on a secure design, for example leaving out important security controls. To achieve a secure design, tools such as threat modeling, secure design patterns and principles, and reference architectures should be used.
- A5:2021—Security Misconfiguration: security misconfiguration usually is a result of insecure default configurations, unnecessary ports or services, misconfigured HTTP headers, and verbose error messages containing sensitive information. All operating systems, frameworks, libraries, and applications must be securely configured, as well as patched and upgraded in a timely fashion.
- A6:2021—Vulnerable and Outdated Components: components such as libraries, frameworks, and other software modules run with the same privileges as the application itself. If a vulnerable or outdated component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
- A7:2021—Identification and Authentication Failures: application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other imple-

mentation flaws in order to assume other users' identities temporarily or permanently. Examples involve allowing weak passwords, permitting brute force or other automated attacks, and weak processes for forgotten passwords.

- A8:2021—Software and Data Integrity Failures: if software and data are transferred between environments, their integrity must be verified, e.g. using signatures. This applies e.g. to moving code along the CI/CD pipeline, downloading updates, or insecure **deserialization**.
- A9:2021—Security Logging and Monitoring Failures: insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, move on to additional systems, and tamper, extract, or destroy data. Most breach studies show that the time it takes to detect a breach is over 200 days, and they are typically detected by external parties rather than by internal processes or monitoring.
- A10:2021—Server-Side Request Forgery (SSRF): in SSRF, an insecure server is used to send HTTP requests to some system that the attacker cannot access directly. For example, the server is induced to connect to an external system and leak information such as login credentials to the attacker. Commonly, an SSRF attack can be performed if the server is trusted by a third system to send requests that contain an URL. In such a case, an attacker may try to modify the URL or some other part of the request, causing the recipient server (which may be the same as the original insecure server) to read or modify internal resources.

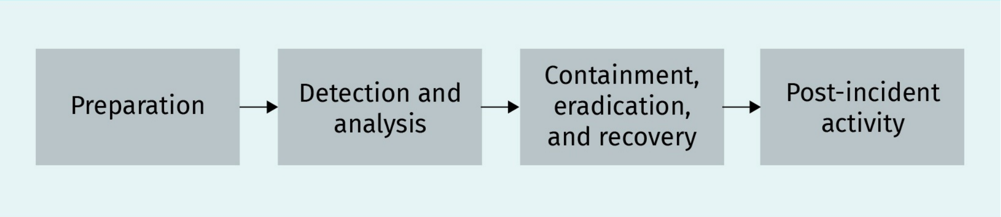
Serialization and deserialization
Serialization is the process of converting objects into a linear (serial) format such as a text string. Deserialization is the process of converting such a linear format back into the object.

OWASP proposes that the Software Assurance Maturity Model (SAMM) should be the prime maturity model for software assurance. It provides an effective and measurable way for all types of organizations to analyze and improve their software security posture. OWASP SAMM supports the complete software life cycle, including development and acquisition, and is technology and process agnostic. It is intentionally built to be evolutive and risk-driven in nature. The most recently developed version of the OWASP SAMM is version 2.0.

Security Incident Management

Every organization and security incident management will work to ensure that the impact of a security incident is reduced to an acceptable level. A security incident response plan includes the steps that are necessary to reduce the impact. This plan should be tested at least annually. The figure below shows the typical life cycle of an incident.

Figure 2: Incident Life Cycle



Source: Created on behalf of IU (2020).

In preparation, an incident response policy is drafted and the response plan and reporting plan are developed. Standard operational procedures (SOPs) define the specific technical processes, techniques, and checklists that might be used during an incident. The structure and staffing of the incident response team is defined, the team is trained, and measures to prevent incidents are taken.

Detecting and analyzing an incident is often the most challenging phase of the incident response process. A security incident and event management (SIEM) system can be used to detect the occurrence of an incident. This is helpful because millions of different events happen every second and teams must focus on the relevant ones in order to avoid event fatigue.

After the incident is identified, measures must be taken to contain it so that it does not spread throughout the organization or to other systems. After these measures have been implemented, eradication may be necessary in order to eliminate components of the incidents, such as deleting a virus. Recovery might include restoring data from backups, installing patches, or changing passwords.

Post-incident reviews and activities include discussing lessons learned and implementing further security controls in order to avoid similar incidents in the future.

1.3 Core Concepts of Data Protection and Privacy

Data protection, also known as data privacy, refers to the conflict faced when protecting the privacy of individuals as well as processing their data. Cyber security is used to protect personal identifiable information (PII) and the security controls are called technical and administrative (or organizational) measures.

Different laws govern data protection worldwide and, as of early 2020, many laws are in the legislative process. Recent additions at the time of writing are the General Data Protection Regulation (GDPR) in the European Union and the Californian Consumer Privacy Act (CCPA) that begins a whole new era of privacy laws in the United States. In particular, GDPR led many countries to start thinking of their privacy laws and many of them, including India, Brazil, and Nigeria, have already enacted new privacy laws or are progressing through the legislative process.

The basic principles of data protection are as follows:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention, and disclosure limitation
6. Accuracy and quality

7. Openness, transparency, and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

1.4 Core Concepts of Cryptography

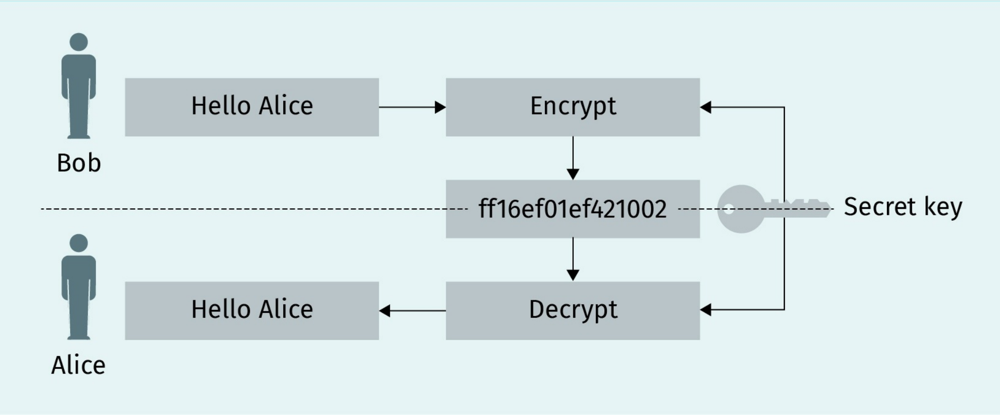
Cryptography is the study of secure communication. Cryptoanalysis tries to find weaknesses in cryptographic algorithms, enabling the decryption of encrypted messages.

We must first define the terminology of cryptography.

1. "Plaintext" is the name of the message before any encryption is applied, when it is still readable by computers or humans.
2. "Encryption" is the process of encoding a message so that it cannot be accessed by anyone without the authorization to do so.
3. "Ciphertext" is the name for the encrypted message.
4. "Cipher" is the algorithm that encrypts and decrypts the plaintext.
5. "Decryption" is the process used to apply the cipher to the ciphertext, resulting in the plaintext.
6. The "key" is the name of the code that, together with the cipher, allows the encryption and decryption of the plaintext and ciphertext.

Kerckhoff's principle states that a cryptographic system must be secure even if everything is known besides the key. Security is not achieved by keeping the cipher algorithm secure but by keeping the key secure (Kerckhoff, 1883). Violations of Kerckhoff's principle are known as "security by obscurity" and have proven to be insecure in the long run. The reason is that known algorithms can be checked, proven, and improved by cryptographic research, and secret algorithms are much more likely to have a weakness.

Figure 3: Symmetric Cryptography



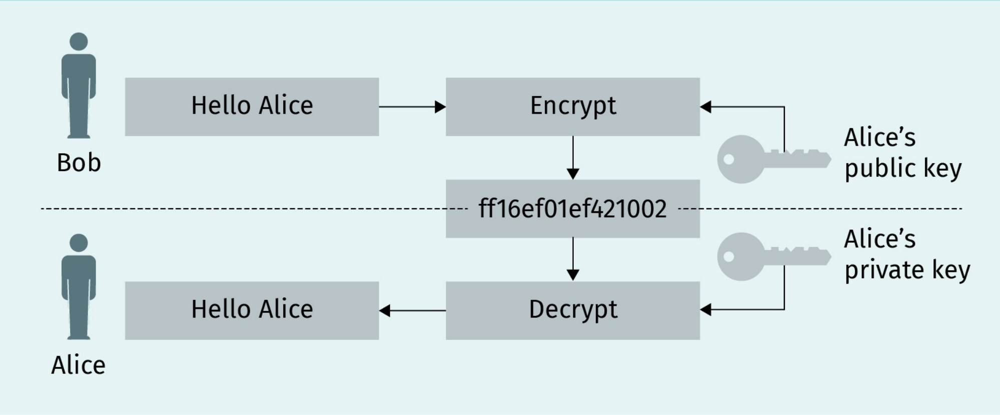
Source: Created on behalf of IU (2020).

It is common to use the names Bob and Alice to represent actors who want to exchange a message. In the figure above, both Bob and Alice know a secret key that they use to encrypt the plaintext "Hello Alice." They exchange a ciphertext and Alice uses the secret key to decrypt the ciphertext into the original plaintext. As only one key is used, this is called symmetric cryptography.

The challenge with symmetric cryptography is exchanging the secret key in a secure manner. In modern scenarios where we want to encrypt every message in a worldwide computer network, exchanging keys would be impossible.

Asymmetric cryptography addresses that issue by giving two keys to each actor: one public key, known to everyone, and one private key that is secret. The public key can be used to encrypt a message to a person and the private key can be used to decrypt it.

Figure 4: Asymmetric Cryptography



Source: Created on behalf of IU (2020).

Asymmetric cryptography can also be used to apply digital signatures and achieve non-repudiation.

Generally, asymmetric cryptography is much slower than symmetric cryptography. Modern cryptographic systems often use asymmetric cryptography to exchange a secret symmetric key and then continue using symmetric cryptography.

Commonly known algorithms for symmetric cryptography are AES or 3DES, and for asymmetric cryptography, RSA or ECC.

1.5 Legal Aspects

Although data protection and privacy laws already exist and are implemented effectively, other legal aspects also influence cyber security.

Cyber Security Laws in the United States

The main regulation in the United States around cyber security is the Federal Information Security Management Act of 2002, which was amended by the Federal Information Security Modernization Act of 2014 (both acts are known as FISMA). The act acknowledges the importance of cyber security in relation to the economic and national security of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source.

FISMA requires federal agencies to manage security based on risk and to have a security program that does the following:

1. Plan for security.
2. Ensure that appropriate officials are assigned security responsibility.
3. Periodically review the security controls in their systems.
4. Authorize system processing prior to operations and periodically thereafter (Hansche, 2005).

The National Institute of Standards and Technology (NIST) publishes documents that provide guidance and clarify how a federal agency can comply with FISMA.

Cyber Security Laws in Europe

The major regulations in Europe are the regulations of the European Union Agency for Cybersecurity (ENISA) and the Directive on Security of Network and Information Systems (NIS).

ENISA (n.d.) is actively contributing to European cyber security policy by supporting Member States and European Union stakeholders concerning a response to large-scale cyber incidents in cases where two or more EU Member States have been affected. This work also contributes to the proper functioning of the digital single market.

ENISA’s approach consists of activities in the following areas:

- recommendations regarding cyber security and independent advice,
- activities that support policy-making and implementation,
- hands-on work where ENISA collaborates directly with operational teams throughout the EU,
- unity of EU communities and coordination of the response to large scale cross-border cyber security incidents, and
- composition of cyber security certification schemes (ENISA, n.d.).

ENISA works together with the national Computer Security Incident Response Teams (CSIRTs).

NIS helps to increase the level of cyber security within the EU. Both digital services providers (DSPs) and operators of essential services (OESs) are in the scope of the directive. OESs provide services such as energy utilities, food supply, and financial services that greatly affect societal and economic activities.

Both DSPs and OESs must report major security incidents to their national CSIRTs.

The NIS follows a risk-based approach requiring both DPSs and OESs to do the following:

- Prevent risks. This includes technical and organizational measures that are appropriate and proportionate to the risk.
- Ensure security of network and information systems. This includes measures to ensure a level of security around the network and information systems that is appropriate to the risks (European Commission, 2016).

SUMMARY

Cyber security and data protection play a vital role in the world today.

Cyber security protects the confidentiality, integrity, and availability of information by using a risk-based approach. Many aspects or domains make up a holistic cyber security program including access control, network security, or the secure development of software.

Cryptography helps to transmit messages secretly. We distinguish between symmetric and asymmetric cryptography. Cryptoanalysis tries to find weaknesses in cryptographic systems.

Data protection and data privacy protect the interests of individuals whenever their personal data is processed.

Many additional legal regulations affect cyber security, including FISMA from the United States, or the NIS regulations and laws that are implemented in the European Union.

UNIT 2

DATA PROTECTION

STUDY GOALS

On completion of this unit, you will have learned …

- the fundamental principles of privacy and data protection that are applicable in all data privacy regulations.
- how ISO 29100 describes the fundamentals of data protection.
- the specifics of data protection regulation in Europe (GDPR).
- an overview of data protection in the United States with a focus on the California Consumer Privacy Act (CCPA).
- an overview of data protection in Asia.

2. DATA PROTECTION

Introduction

Data protection and data privacy play an increasingly important role in our personal lives, as well as in the processing of data in our organizations. In 2019, Shinzo Abe, Japan's prime minister, made data privacy a priority for the G20 summit hosted by Japan. Many developed and developing countries have already enacted new data protection regulations or are currently implementing legislative processes to enact them. This shows that regulations are an important factor to consider in the 21st century. Protecting the privacy of every individual is an important ethical requirement, so societies all over the globe are demanding further protection.

Global and holistic concepts define data protection and set principles that feature in every national and international regulation.

2.1 Basic Concepts of Data Protection (ISO/IEC 29100, Privacy by Design)

Data Privacy versus Data Protection

Data privacy and data protection, though connected, are commonly recognized all over the world as two separate rights. In many countries, they are considered vital components of a sustainable democracy.

In Article 1 of the Universal Declaration of Human Rights (United Nations, 1948), human dignity is recognized as an absolute fundamental right. These notions of dignity, privacy or the right to a private life, autonomy, or the right to be left alone, plays a pivotal role. Privacy is not only an individual right but also a social value.

Historically, in other parts of the world, such as the United States, privacy has often been regarded as an element of liberty, for example, the right to be free from intrusions by the state.

Privacy—A Fundamental Right

Almost every country in the world recognizes privacy in some way, be it in their constitution or in other provisions.

Moreover, privacy is recognized as a universal human right, while data protection is not—at least, not yet.

The right to privacy or a private life is enshrined in the Universal Declaration of Human Rights (Article 12) (United Nations, 1948), the European Convention on Human Rights (Article 8) (European Court of Human Rights, 2013), and the European Charter of Fundamental Rights (Article 7) (European Union, 2000).

What Is Data Protection?

Data protection applies to any information relating to an identified or identifiable natural (living) person including names, dates of birth, photographs, video footage, email addresses, telephone numbers, and more.

Different regulations have different names for these aspects, e.g., data subjects in the EU, PII principals in international standards such as ISO 27701 and ISO 29100, and consumers in California (International Organization for Standardization, n.d.). This course book will use the term “PII principals” to ensure the consistency and neutrality of certain specific regulations.

The term used for the data about a PII principal will be Personal Identifiable Information (PII) for the remainder of this unit. This is also a term used in many regulations and in the relevant ISO standards.

The notion of data protection originates from the right to privacy—both are instrumental not only to the preservation and promotion of fundamental values and rights, but also to the exercising of other rights and freedoms such as free speech or the right to assembly.

Data protection includes the rights of the PII principal that consist of fair processing, transparency, and certain rights to access or change PII.

Data protection has precise aims to ensure the fair processing (collection, use, and storage) of personal data by both the public and private sectors.

Principles of Data Protection

The following principles are guiding all global data protection regulations. They can be found in international standards, specifically in ISO/IEC 29100:2011 Information technology—Security techniques—Privacy framework (2011); ISO/IEC 27701:2019 Security techniques—Extension to ISO/IEC 27001 (2019); and ISO/IEC 27002 for privacy information management—Requirements and guidelines (2019).

PII controllers and PII processors

PII controllers determine the means and purposes of processing PII. Controllers must ensure that applicable laws are adhered to, and they are obliged to demonstrate compliance. A PII processor follows the instructions of a PII controller in order to process PII. Under many regulations, the relationship between a controller and processor requires a written contract.

Consent and choice

Opting in or opting out
Opt-in: default value is no, but principals may allow that their data are processed. Opt-out: default value is yes, but principals may object to their data being processed.

PII principals should have the choice of whether their data is processed. That choice should be presented upfront, and the consequences of **opting in or opting out** should be made clear. The consent given by the PII principals can be withdrawn at a later stage. This principle is not contrary to the fact that, in many cases, processing is based on existing contracts, legal requirements, or other legal means. It applies to cases where consent is the legal basis for the processing of PII.

Example: Before using cookies to track a user's behavior on a website, permission should be requested and consent should be obtained for the implementation of cookies on the user's desktop.

Purpose legitimacy and specification

All processing of PII must be compliant with applicable laws. The purpose of data processing must be communicated to the PII principals upfront, but it should be communicated again if the purpose changes over time.

Example: If data was collected by a Web shop for the purpose of delivering the ordered products to the PII principal, the purpose should not be changed without obtaining further consent and giving the participants information about their being part of a big data analysis.

Collection limitation

The collection of PII should be limited to what is strictly necessary for the purpose defined and should be within the limitations of applicable laws.

Example: A Web shop might need to check if there is an age requirement that must be met in order to be permitted to buy products such as alcohol. It might be tempting to record the date of birth but that is not strictly necessary. Simply recording that an age check was done would fulfill the requirement.

Data minimization

Data minimization is related to collection limitation but goes further, looking at the processing after the initial collection of PII. It means that the processes and systems for processing PII must limit the number of stakeholders that have access to or the ability to process data; ensure that PII can be accessed on a need-to-know basis only; and offer options that do not require the use of PII. Also, PII must be deleted when there are no longer legal requirements stating that it should be stored and it is not needed for any further purpose.

Example: In a hospital, it might be practical for all medical personnel, nurses, doctors, and administration staff to have access to the patients' PII. However, on a need-to-know basis, doctors and nurses should only have access to the data of their own patients, and the administration staff only needs data that is relevant for coping with insurances and invoices.

Use, retention, and disclosure limitation

Data must not be retained forever. This principle is about retaining data for a defined purpose, but only for as long as it is required by the organization and by law. After that period, PII should be destroyed. An example is locking records. This is necessary when the processing of data is no longer required but applicable laws still require that the data is kept for archiving purposes. In this case, the record must be locked, which means that it cannot be used anymore outside of the access allowed by the law.

Example: The purpose of keeping payroll data is limited to the time that an individual is employed by an organization. Applicable laws such as social security laws, labor laws, or taxation regulations might require the data to be archived for several years. The records must be locked after the individual leaves the company, and the data must be destroyed when the limits set by the other laws are reached, e.g., after six or ten years.

Accuracy and quality

The PII process has to be accurate and completed to a degree that it can be adequately used for the purpose defined. If PII is collected from a source that is not the PII principal, the reliability must be ensured. The accuracy and quality of the data should be checked regularly.

Example: A credit scoring system relies on accurate data from an individual's credit history. If that history is not correct, e.g., a loan which was repaid is recorded as defaulted, the individual might be refused a loan that they were eligible to get. Both the individual and the loan association would be damaged by this inaccuracy of data.

Openness, transparency, and notice

This principle means that information about the processing of PII and the purposes and means for doing so should be provided to the PII principals. In the interest of transparency, this notice should be easily readable, especially if a processing activity includes decision-making based on the PII.

Example: If an individual uses an internet search engine, the data of the individual are processed. The search engine provider publishes a data privacy notice that explains which data are processed and how they are processed. This notice includes information that influences the search results and advertisements shown to the individual.

Individual participation and access

Individuals have many rights, including the right to access their data, change inaccurate data, delete or lock the data, and easily assert these rights. In some legislations (e.g., GDPR and CCPA), they also have the right to portability, making the data available in an electronic, standardized form. Often CSV, JSON, or XML formats are used.

Example: Individuals can ask an online shop to provide them with their data. If they decide not to be targeted any more by newsletters, they can have their data record locked. A deletion can take place when other laws do not require the records to be archived any longer.

Accountability

There is a duty of due care stating that measures must be taken by an organization to ensure the protection of PII. Accountability means that an organization must be able to prove its compliance. Data privacy policies and processes are documented. Contractual agreements provide safeguards when transferring data to third parties. When a breach occurs, the individuals must be informed about it. If privacy authorities exist, they have certain audit rights as well as the right to be informed about the processing of PII.

Example: In Israel, the Protection of Privacy Law requires an organization that processes more than 10,000 personal records in a database to register this database with the national authority. This registration includes documentation of the nature of the database, the processing, and the security measures taken to protect the database.

Information security

PII must be protected, and the CIA (confidentiality, integrity, and availability) of information has to be assured by the controller. The precautions taken are usually based on a risk assessment and a catalog detailing which steps should be implemented. It includes access control on a need-to-know basis, encryption of data, relevant physical and network controls, and other security measures.

Example: A database containing PII should be encrypted, and passwords of user accounts should be hashed and salted to protect the confidentiality and integrity of the database.

Privacy compliance

An organization must be able to demonstrate compliance by having independently verified internal controls in place. An adequate and documented risk management system is a way to show privacy compliance.

Example: Internal and external audit programs, including certification by accredited certification bodies, are ways to show compliance.

2.2 Data Protection in Europe: The GDPR

Within Europe, the major international organization is the European Union (EU). The General Data Protection Regulation 616/679 (GDPR) is directly applicable in all EU Member States and the states belonging to the European economic area. It is accompanied by the ePrivacy Directive (ePD) 2002/58/EC, which is planned to be replaced by an updated regulation (note that the legislative process was postponed several times and proposals were rejected). The GDPR replaces the former directive 95/46/EC concerning data privacy. As a regulation, the GDPR is directly applicable by law in the Member States and does not require a local law to be effective. However, the Member States implemented local privacy legislations to support the GDPR. In addition, several other national laws are applicable, including state laws, church laws, labor laws, and contractual agreements (for example, those between trade unions and employer organizations).

The GDPR is recognized worldwide as the benchmark for privacy regulation. Upcoming regulations in several countries, including the United States, India, Brazil, and Nigeria, are based on the same principles and structured in a similar way.

The GDPR consists of 99 articles in 11 chapters. One hundred and seventy-three recitals help with the interpretation of the law.

Scope of the GDPR

The material scope of the GDPR covers all personal and material relationships of an identified or identifiable natural person. PII must be processed either in an automated way, a semi-automated way, or as a paper-based archive. There are few exceptions to the material scope of GDPR, including private households, law enforcement activities, and data usage for national security. The GDPR applies to both controllers and processors.

The territorial scope follows the market principle. It applies to all organizations established in the EU, and to organizations that track EU citizens and offer services or products within the EU. As the EU is the largest market in the world, this makes the GDPR applicable to many organizations operating outside of the EU.

Special Categories of Data

Article 9 GDPR (European Union, 2018) defines special **categories of data**. The processing of those is only allowed if there is a special legal requirement or if the individual gave consent. These legal requirements are as follows:

Categories of data
Note that sensitive information is sometimes indirectly included in the data, for example, an HR database requiring the name of someone's partner could reveal their sexual orientation.

- race and ethnic origin,
- religious or philosophical beliefs,
- political opinions,
- trade union memberships,
- biometric data used to identify an individual,
- genetic data,
- health data, and
- data related to sexual preferences and/or sexual orientation.

If special categories of data are processed, the security of the processing must account for the high risk of that data.

Accountability in GDPR

To demonstrate accountability, GDPR requires organizations to maintain a record of processing activities (ROP). Article 30 GDPR (European Union, 2018) describes what a record of processing activities must include. The authorities can ask for the ROP when auditing organizations. Organizations must also implement security which includes the CIA plus resilience as a fourth factor of security. During implementation, security risk needs to be considered. Article 25 GDPR (European Union, 2018) states that the following criteria should be considered when carrying out the risk assessment:

- state of the art,
- costs of implementation,
- nature, scope, context and purposes of processing, and
- risk of varying likelihood and severity to the rights and freedoms of natural persons.

In case of a planned activity that poses a high risk to the rights and the freedom of a person, a data protection impact assessment (DPIA) must be done (European Union, 2018). National authorities and the European Data Protection Board (EDPB) clarify that some activities always require a DPIA. Examples of those are CCTV and credit scoring.

Privacy by design and by default are principles that an organization must obey. It means that privacy is not an afterthought, but rather needs to be implemented during the design phase of processes and tools. Privacy by default means that privacy friendly settings must be the default option. An example is the settings of cookies that should only be pre-tagged if they are essential to the functioning of a website, whereas all other kind of cookies must be untagged by default.

Lawfulness of Processing

According to Article 6 GDPR, there are exactly six reasons that make the processing of PII lawful (European Union, 2018). They are as follows:

- The PII principal (data subject) has given consent.
- Processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller.

It is important to understand the legal basis when PII is processed. Consent is often misused as another legal basis, but that consent must be freely given and can be withdrawn at any time. The vital interest legal basis is interpreted in a way that applies to emergency situations. Not every health related activity falls under this legal basis.

Privacy Compliance

Compliance to the GDPR is both self-controlled and controlled by supervisory authorities. A crucial role in controlling compliance is played by the Data Protection Officers (DPOs). They are employed by the organizations that are processing PII, and they monitor and audit the compliance with GDPR. They also give advice and handle the complaints of the PII principals. To ensure that they can act independently, a DPO must not receive any direct instructions. The DPO must report to the highest management level in an organization.

External control is ensured via the supervisory authorities. The Member States of the EU have set up these authorities on either a country or a state level. They collaborate via the European Data Protection Board, formerly known as the Article 29 group. They can gather information, audit organizations, handle complaints, and request the mitigation of issues found. They can also issue fines for non-compliance. The fines should be effective, proportionate, and dissuasive. The fines are capped at a maximum of four percent of the worldwide revenue of an organization or EUR 20 million.

Article 42 GDPR (European Union, 2018) facilitates a certification that could be obtained to show compliance. At the time of writing, no approved certification scheme exists. Note that a certification against ISO 27001 in conjunction with ISO 27701 will not be an Article 42 GDPR certification as those are based on ISO 17021, whereas the Article 42 GDPR certification will be based on ISO 17065.

Rights of the Data Subjects

Chapter 3 of the GDPR (European Union, 2018) notes the rights of the data subject (PII principal). They are

- transparency about the processing of data and the rights of the individual,
- information and access to personal data,
- rectification and erasure, and
- the right to object and automated individual decision-making.

In case of damages occurred, the data subjects can hold an organization liable. The liability is unrestricted and based on the damages caused, e.g., by a data breach.

Data Transfers

Data transfers between controllers and processors, and between controllers and controllers, require a written contract, known as a Data Processing Agreement (DPA). Article 28 GDPR (European Union, 2018) requires eight topics to be added to the DPA. They are as follows:

- The processor only agrees to process personal data if they have received the written instructions of the controller.
- Everyone who comes into contact with the data is sworn to confidentiality.
- All appropriate technical and organizational measures are used to protect the security of the data.
- The processor will not subcontract to another processor unless instructed to do so in writing by the controller, in which case, another DPA will need to be signed with the sub-processor (pursuant to Sections 2 and 4 of Article 28).
- The processor will help the controller uphold their obligations under the GDPR, particularly concerning data subjects' rights.
- The processor will help the controller maintain GDPR compliance with regard to Article 32 (security of processing) and Article 36 (consulting with the data protection authority before undertaking high-risk processing).
- The processor agrees to delete all personal data upon the termination of services or return the data to the controller.
- The processor must allow the controller to conduct an audit and will provide whatever information necessary to prove compliance.

A data transfer can also take place between parties outside of the European Union. In this case, specific additional safeguards need to be in place. The most common safeguards are as follows:

- Adequacy decisions: The EU Commission decides that the level of data protection in a third country is at a level that is acceptable to the EU. Current big economies that have obtained an adequacy decision are Argentina, Japan, Canada (private sector). The former adequacy decision for the United States (Privacy Shield) was invalidated by a decision of the European Court of Justice in July 2020.
- EU model clauses: The model clauses or standard contractual clauses issued by the EU. If a processor or controller outside the EU signs and obeys them and the remaining risk is considered acceptable as shown by a transfer impact assessment (TIA), the data can be transferred. This is the most common way to safeguard data transfers to third countries.
- Binding corporate rules: An enterprise can obey binding corporate rules that have been approved by the national authorities of the country where its EU headquarters are based. If those are approved, data can flow inside this enterprise. Binding corporate rules have no impact on relationships outside of that enterprise.

Data Breaches

Whenever a data breach occurs, the organization has 72 hours from the time that the breach was discovered to inform the supervisory authority. If the risks to the rights and freedoms of the individuals is high, the affected individuals must also be informed about the breach.

2.3 Data Protection in the United States

At the time of writing, data protection laws in the United States are changing significantly. At least 17 states are carrying out legislative processes to enact new data protection laws, California being the first with the Californian Consumer Privacy Act (CCPA). Both the Republican and the Democratic parties have proposed new data protection laws at the federal level. Both proposals refer to the European GDPR and are aligned towards similar principles. The current legislation is mostly dependent on the state and stems from consumer rights. Also, sector-specific laws, such as the Health Insurance Portability and Accountability Act (HIPAA) for the health sector or the Fair Credit Reporting Act (FCRA) for the banking sector, exist and play a large role in their respective sectors.

The Federal Trade Commission (FTC), an important federal agency, has worked since the 1970s to protect the privacy of consumers from the United States. It does not play the same role as a privacy authority in other states; however, the proposed laws on a federal level try to place the supervisory function with the FTC, emphasizing the role it plays in relation to privacy in the United States.

In this section, we will focus on the CCPA regulation, and HIPAA as examples of privacy regulations in the United States. We will also cover the role of the FTC. In the absence of a federal law it is not possible to provide a complete and holistic overview, but the choice allows the reader to understand what privacy currently means in the United States.

The Role of the FTC

When companies tell consumers that they will safeguard personal information, the FTC can take legal action to make sure that companies live up to these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts or practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security (Federal Trade Commission, n.d.).

Hence, the FTC plays a role in protecting consumers' privacy. An example is the case against YouTube (FTC no. 172 3083) (Federal Trade Comission, 2019) where the FTC issued them a fine of $170 million for collecting the information of minors without prior consent from their parents.

Californian Consumer Privacy Act

On January 1st, 2020, the Californian Consumer Privacy Act (CCPA) was enacted, beginning the modernization of United States privacy laws. The title of the CCPA is a bit misleading because it does not only protect consumers, but all California residents, their devices, and their households. California represents about 12 percent of the United States population and is the seventh largest economy in the world. Hence, the CCPA has national and international influence.

To be under the scope of the CCPA, an organization must meet at least one of the following criteria:

- Annual gross revenue of $25 million
- Buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices
- At least 50 percent of annual revenue from selling consumers' personal information (California Legislative Information, 2018)

The PII principals are considered to be consumers under CCPA and have the right to

- know what PII is being collected about them.
- access their PII in a readily useable format.
- know whether their personal information is being sold or shared, and if so, with whom.
- opt out of the sale of their PII (opt in, in cases of minors).
- equal service and price regardless of exercising individual rights.
- deletion of their PII upon request.

Data requested is from the preceding 12 months, and individuals can make up to two requests in a 12-month period. An organization has to set up a free number to call and an email address or Web form where consumers can request that any of their rights are enacted. The law uses the term "personal information" broadly, so traditional information, as well as behavior or preference-based information, falls under it. The CCPA defines the term "selling" in a broad sense, and further clarifications are expected. It includes selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating PII to another business or third party for monetary or other valuable consideration. If a company is selling data, it must place a link on its Web page where individuals can opt out of selling their data. The default option can be opt out for adults, but for minors, the default is opt in.

The CCPA uses the terms "service providers" for controllers and "third parties" for processors. To enforce the act, the California attorney general can issue fines of up to $7,500 per violation. It is not yet clear how the violations are counted. If they result from a failure to maintain reasonable security, private right of action is limited to $750. These are normally enforced during a class action. Keep in mind that the private damages are per record, so if 100,000 records are breached and all affected consumers take part in the class action, the liability could reach $75 million. Several amendments were enacted to clarify the scope of CCPA or to put a moratorium on the scope. Important ones are Assembly Bill 25 (AB-25) that exempts employee data from the scope for one year and AB-1355 for a moratorium on B2B-related PII. The CCPA does not require an organization to have a data protection officer (DPO).

Health Insurance Portability and Accountability Act

Due to its sensitive nature, a federal legislation on health privacy was enacted in 1996. This is the Health Insurance Portability and Accountability Act, known as HIPAA. Since then, it has regularly been updated to cope with technological progress and changes in scope. The PII principals are called "patients" in HIPAA, and the Act safeguards patient data in all forms, such as health plans, healthcare clearinghouses, and healthcare providers (including doctors, nurses, hospitals, and therapists). Patient information in oral, written, and electronic form is protected. This includes demographic information that is tied to the identity of the patient. Patients have the right to access their data. Organizations can charge a reasonable amount to provide this information.

The privacy rules of HIPAA ensure that the policies are applied in a manner that ensures proper protection of data and does not leave room for mistakes. It sets clear rules for medical care organizations concerning the way that patient data is governed. Written permission is required whenever patient data is disclosed. HIPAA requires administrative, physical, and technical controls, policies, and procedures to guarantee the CIA of electronic personal health information (ePHI). Examples of required administrative measures are the implementation of risk management, or a data backup plan. Examples of required physical safeguards are a facility security plan or secure disposal of media. Examples of technical safeguards are authentication or emergency access procedures.

Penalties are enforced in the case of non-compliance with HIPAA. For a laptop theft including unencrypted patient data at a hospice in Northern Idaho, a penalty of $50,000 was issued. All together, fines have reached more than $36 million so far. The fines are limited to $1.5 million per year per institution. The fines are enforced by the Department of Health and Human Services' Office for Civil Rights (OCR) and state attorneys general. The United States Food & Drug Administration (FDA) checks medical devices before they reach the market, and privacy is considered in that process (United States Food & Drug Administration, 2018).

2.4 Data Protection in Asia

There is no consistent data privacy law in Asia defined by any multinational organization such as ASEAN, the largest trade organization in Asia. Each country in Asia has its own data privacy regulations. In this section, we will examine the situation in India and Singapore, focusing on two important economies in the region.

Data Privacy in India

Right now, India has constitutional right of privacy but no privacy law. Privacy law only exists for case law and does not follow a concise structure like in the previously described legislations. In 2018, the Indian Personal Data Protection Bill was proposed. At the time of writing, this bill is still in the legislative process, and several changes and amendments have been discussed. Until the law is enacted, privacy regulation in India remains a difficult subject.

The Information Technology Act (Parliament of India, 2000) has two sections concerning privacy. Section 43A requires an organization to implement reasonable security practices for sensitive personal data and to compensate an individual when a breach occurs. Sensitive personal data are passwords, health records, sexual orientation, biometrics, and financial information. Section 72A covers punishment such as fines and imprisonment of up to three years, for people who cause data breaches. The same law gives the Indian government a lot of power to interfere with the data of its citizens. It permits the interception, monitoring, and decryption of digital communication and allows the government to set national encryption standards. There are governmental projects that intercept phones and internet connections. The Indian National Intelligence Grid (NATGRID) project is an example of this, combining several databases with citizens' data and making it easily accessible to intelligence agencies. The proposed privacy laws would make privacy a more fundamental right and protect the citizens from state surveillance.

Data Privacy in Singapore

In Singapore, data privacy is regulated via the Personal Data Protection Act (PDPA) from 2012. Several regulations were added in 2013 to govern the enforcement of the Act detailing special provisions regarding phone calls and exemptions therefore building a comprehensive privacy framework in Singapore (Personal Data Protection Commission Singapore, n.d.).

The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure, and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use, or disclose personal data for legitimate and reasonable purposes.

The PDPA provides for the establishment of a national Do Not Call (DNC) Registry. The DNC Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organizations.

The scope of the PDPA covers all personal data with the following four exceptions:

1. Any individual acting on a personal or domestic basis
2. Any employee acting in the course of his or her employment with an organization
3. Any public agency or organization acting on behalf of a public agency in relation to the collection, use, or disclosure of the personal data
4. Business contact information

The Act justifies the Personal Data Protection Commission, a privacy authority that has the responsibility to administer the Act. Besides giving advice, the Commission also enforces the Act and monitors its compliance.

Generally, the Act requires consent. The law defines a long list of activities where no consent is required. Those are set in the second schedule of the Act and include things like the interest of the individual, artistic purposes, and more.

The law gives individuals the right to access and correct their data for accuracy, protection, and adequate retention. In case of disputes, the commission helps the individual and the controller to go through a mediation process to solve the conflict.

The possible punishments for non-compliance range from fines to three years in prison. So far, many fines are in the region of 5,000—100,000 SGD.

The PDPA requires an organization to have a data protection officer (DPO). The DPO has the following obligations (Personal Data Protection Commission Singapore, n.d.):

- ensure compliance of PDPA when developing and implementing policies and processes for handling personal data,
- foster a data protection culture among employees and communicate personal data protection policies to stakeholders,
- manage personal data protection related queries and complaints,
- alert management to any risks that might arise with regard to personal data, and
- liaise with the PDPC on data protection matters, if necessary.

In Singapore, the privacy law is currently changing. In March 2019, the PDPC stated that breach notifications might become mandatory and that individuals should have greater control over data transfers to third parties. A draft bill is expected in 2020.

SUMMARY

Privacy and data protection are not the same. Regulations all over the world follow similar principles in their data protection regulation, but there are also significant differences. In Europe, the GDPR sets clear and strict guidelines, whereas the regulations in the United States are more diverse and heavily dependent on the state, the sector of industry, and the scope of processing.

In Asia, the situation is even more diverse as each country has its own data protection regulations. Some countries, such as India, are still in the middle of a legislative process, whereas others, such as Singapore, have more mature regulations.

Due to the high amount of fines and extraterritorial scope, the GDPR sets the worldwide benchmark for privacy regulations and is applicable to many organizations.

In almost all countries, privacy laws are emerging or being modernized, so tany observer of privacy laws must watch carefully for new developments.

UNIT 3

APPLYING DATA PROTECTION

STUDY GOALS

On completion of this unit, you will have learned …

- how to practically apply data protection regulations in several scenarios.
- what anonymity is and how it can be achieved.
- the challenges faced when using PII in big data scenarios.
- how online marketing can work in compliance with data protection.
- the impact of data protection on cloud computing.

3. APPLYING DATA PROTECTION

Introduction

In this unit, we will examine ways to implement laws and regulations that govern privacy and data protection. Practice shows that it is not as easy as it sounds to implement the requirements of the law. Recent reports about the influence of personal data on elections and the availability of location data show that implementing adequate controls around privacy is failing in some areas. We are going to examine several ways to achieve privacy and the challenges in doing so.

3.1 Anonymity and Pseudonyms

Anonymity is a situation where the identity of the person acting is unknown. In information technology, it refers to data where it is impossible to identify the individual whose data is processed. One challenge when dealing with anonymity is that it is often possible to re-identify individuals. Some examples include

- IP addresses assigned by Internet Service Providers (ISPs) who can identify individuals,
- location data history, which can often reveal an individual,
- unique identifiers such as social security numbers, customer numbers, or personnel numbers, that can be mapped to an individual, and
- statistical data filtering, which can often reveal the identity of an individual.

These challenges have triggered research in the area of anonymity and how to achieve it.

k-Anonymity

k-anonymity is a concept that manages the conflict of using data and, at the same time, protecting the privacy of the individuals involved with the data. This compromise is achieved by making the data less accurate. The following example will show how it works. Assume that we have a list of voters in an employee satisfaction survey. We want to give managers enough information to act on the feedback but, at the same time, ensure that they cannot determine who provided the feedback. The initial, non-anonymized feedback table looks like this:

Table 1: Non-Anonymized Feedback Table

Name	Age	Country	Gender	Feedback
Susan	24	USA	Female	Bad
Martin	27	Germany	Male	Good
Rachel	20	Israel	Female	Bad

Name	Age	Country	Gender	Feedback
Ramu	28	India	Male	Medium
Ralf	32	USA	Male	Good
Natalie	33	Israel	Female	Medium
Miriam	33	Germany	Female	Good
Sven	34	Germany	Male	Medium
Aurelie	30	Belgium	Female	Medium
Eva-Maria	29	USA	Female	Medium

Source: Created on behalf of IU (2020).

The challenge with this kind of data is that even though the name is removed, filters relating to country or age could still indicate who gave the feedback. Upon seeing the age and country of the individuals, it would be easy to get the feedback of Rachel and Natalie.

Hence, two methods are applied:

1. Suppression: Attributes are removed completely, in this case the name and the country.
2. Generalization: The process of replacing specific data with broader categories. An example of this is demonstrated below in the age field.

Table 2: 2-Anonymity Feedback Table

Name	Age	Country	Gender	Feedback
*	< 25	*	Female	Bad
*	25-35	*	Male	Good
*	< 25	*	Female	Bad
*	25-35	*	Male	Medium
*	25-35	*	Male	Good
*	25-35	*	Female	Medium
*	25-35	*	Female	Good
*	25-35	*	Male	Medium
*	25-35	*	Female	Medium
*	25-35	*	Female	Medium

Source: Created on behalf of IU (2020).

This dataset achieves 2-anonymity because for any combination of age and gender, there are always at least two rows with the same attribute values.

This is still not ideal; in the example, even without knowing which of the two females in the <25 age group is contained in which row, it is still clear that both gave the feedback “bad”.

l-Diversity

l-diversity (often written as ℓ-diversity) is an extension of the *k*-anonymity model that addresses the problem shown in the example. For a dataset to be *l*-diverse, it must be *k*-anonymous for some value $k \geq l$, and for any set of rows containing the same combination of identifying attributes (in the example: age and gender), there must be at least *l* different values in the sensitive attribute (in the example: feedback). Again, this is a compromise between privacy and still being able to use the data. A 3-diverse table would look like the one demonstrated in the following figure.

Table 3: 3-Diverse Feedback Table

Name	Age	Country	Gender	Feedback
*	2*	*	Female	Bad
*	2*	*	Female	Medium
*	2*	*	Female	Bad
*	2*	*	Male	Good
*	2*	*	Male	Medium
*	2*	*	Male	Good
*	3*	*	*	Medium
*	3*	*	*	Medium
*	3*	*	*	Good
*	3*	*	*	Medium

Source: Created on behalf of IU (2020).

Differential Privacy

Differential privacy changes data so that it still can be used statistically, but the privacy of individuals is maintained. A common example is to survey individuals if they possess a certain trait. Everyone tosses a coin before answering. If the coin toss reveals heads, the person answers with the truth. If not, the person answers with “yes.” This way, the overall statistics of the dataset are still useful, but it makes it impossible to reveal whether the answer “yes” by a certain individual was given because it is true or because of the coin toss.

The definition of differential privacy uses the parameter ε to measure the privacy of a dataset.

Differential privacy adds random noise to a dataset in order to achieve the requested level of privacy. These can be random dummy records that are added or random changes to datasets.

Pseudonymization

In some use cases, anonymizing data is not acceptable since one does not want to completely lose the relationship from data to the people concerned even though most of the time, it is not needed. For example, in a long-term medical study one does not need to know the identity of the patients whose data are processed, but one may want to be able to assign new data collected a year later to the same patients.

This can be achieved by pseudonymizing the data which is a form of processing of personal data which ensures that, although persons can still be identified using the data, this is only possible using additional information that is kept separately, with restricted access. For example, the data may contain a random number (the pseudonym) instead of the name of the person, and the table relating numbers and names is kept confidential.

From a data protection perspective, pseudonymized data are very different from anonymous data. Pseudonymizing data is a measure that can help to protect personal data adequately and therefore is recommended in regulations such as GDPR or the PCI DSS standard used for credit card data. (Note that in PCI DSS, this approach is called masking.) Nevertheless, pseudonymized data are still considered personal data and therefore have to conform to relevant data protection regulations. Anonymous data, on the other hand, are not considered personal data and data protection regulations are therefore not applicable.

3.2 Data Protection in Data Science and Big Data

The terms big data, data science, and artificial intelligence are often used together to define similar things. As these concepts have similar challenges when it comes to data protection, we will use the following definitions: Big data are high-volume, high-velocity, and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision-making (Big Data, n.d.).

Artificial Intelligence (AI) is a subdiscipline of computer science which is concerned with the investigation of the mechanisms of intelligent human behaviour. It tries to implement into IT system behaviour that would be considered “intelligent” in humans.

Throughout this unit, we will use the term “big data,” but that also includes artificial intelligence and data science applications. The following aspects make this kind of processing special:

- use of algorithms,
- opacity of the processing,
- tendency to collect all of the data,
- repurposing of data, and
- use of new types of data.

Hence, from a data protection perspective, several principles are violated and need to be taken care of in order to ensure compliance with privacy regulations. There are many benefits that come from these new forms of processing. Examples include targeting customers more specifically, ensuring more adequate personalized resources are produced for education, and making transportation routes more efficient. There are also a lot of risks as these tools can lead to unintended outcomes. For example, some algorithms have discriminated based on gender during job application processes or discriminated based on race when it came to determining prison sentences. The ICO (Information Commissioner’s Office), the data protection authority in the United Kingdom, requires organizations to consider the following aspects when using big data (Information Commissioner’s Office, 2017). This list provides a summary of these requirements.

Intrusive effects
These can be credit scores or decisions regarding job applications.

1. Fairness
   a) Some types of big data analytics, such as profiling, can have **intrusive effects** on individuals.
   b) Organizations need to consider whether the use of personal data in big data applications is within people’s reasonable expectations.
2. Conditions for processing personal data
   a) Obtaining meaningful consent is often difficult in a big data context, but novel and innovative approaches can help.
   b) Relying on the legitimate interest condition is not a soft option. Big data organizations must always balance their own interests against those of the individuals concerned.
3. Purpose limitation
   a) The purpose limitation principle does not necessarily create a barrier for big data analytics, but it means an assessment of the compatibility of processing purposes must be completed.
4. Data minimization and retention
   a) Big data analytics can result in the collection of personal data that is in excess of what is needed for the processing purpose. Retention periods must not be extended to ensure that big data analysis can take place.
5. Accuracy
   a) There are implications regarding the accuracy of personal data at all stages of a big data project: collection, analysis, and application.
   b) Hidden biases in datasets can lead to inaccurate predictions about individuals.

6. Rights of the individuals
    a) The vast quantities of data used in big data analytics may make it more difficult for organizations to comply with the right of access to personal data.
7. Accountability
    a) Machine learning algorithms have the potential to make decisions that are discriminatory, erroneous, and unjustified.
    b) Data quality is a key issue for those with information governance responsibilities in a big data context.
8. Data controllers and processors
    a) Organizations outsourcing analytics to companies specializing in AI and machine learning need to carefully consider who has control over the processing of any personal data.
9. Anonymization
    a) Often, big data analytics will not require the use of data that identifies individuals, hence anonymization can mitigate a lot of the risks.
10. Privacy by design and by default
    a) Embedding privacy by design solutions into big data analytics can help to protect privacy through a range of technical and organizational measures.
11. Algorithmic transparency
    a) Auditing techniques can be used to identify the factors that influence an algorithmic decision.
    b) A combination of technical and organizational approaches to algorithmic transparency should be used.

Having these measures in mind during implementation and design helps an organization to achieve compliance and process PII in a fair and ethical way.

3.3 User Tracking in Online Marketing

Tracking in online marketing refers to logging a user's activity on the Web. Tracking is used to determine the success of marketing campaigns, to associate clicks with the affiliate that helps to fund many websites, and to check whether or not a website can be used.

Tracking
Advertisements on the web are targeted at you based on previous interest in a topic. This is achieved via tracking and often via cookies.

Tracking provides the following information:

- from where a user accesses a Web page,
- how often pages are accessed,
- how long a user stays on a certain page, and
- where users go when they leave the site.

The privacy risk is that via tracking the behavior of users, this behavior can be steered. Cambridge Analytica used tracking to issue ads in a political campaign that included fake news, but these ads were extremely difficult to detect as they only reached a small number of individuals (Hern, 2018). Sensitive personal data can also be revealed by understanding the browsing habits of an individual.

Different tools are used to track users' behavior:

- First-party cookies are stored by the domain (website) that a user is visiting directly. They allow website owners to collect analytics data, remember language settings, and perform other functions.
- Third party cookies are created by domains outside of the one an individual is visiting directly, hence the name "third party." They are used for cross-site tracking, retargeting, and ad-serving.
- Cross-device tracking is a technique used to track a user across the different devices that they use.
- Fingerprint tracking uses certain characteristics of a browser (version, fonts installed, hardware details, etc.) to identify a user. Nothing needs to be stored on the device of the user.
- Common IDs that users log in to, such as Google ID or Apple ID.
- Advertising IDs allow tracking on mobile devices.
- Web beacons or tracking pixels can show that a user has accessed certain content.

There is a lot of ongoing discussion about the legality of Web tracking in the European Union under GDPR. The CCPA may also change the situation in California in the future. The advertising industry argues that it is their legitimate interest, inherent in their business model, and also beneficial to the users to use tracking technology. Privacy advocates and consumer groups argue that this is not the case and a user may only be legally tracked if they have provided valid consent. A recent case (October 1st, 2019, Case C-673/17) at the European Court of Justice made a preliminary ruling between Planet49, an advertisement organization, and a German consumer organization. The case makes it clear that cookies that are not strictly necessary must be untagged according to the privacy by default principle (Infocuria, 2019).

A typical cookie banner gives the users choices for each category of cookies. Buttons can be pushed to accept all cookies or to save certain settings. Necessary cookies are usually pre-tagged. Users get an explanation about the different categories of cookies. This is done in language that users can understand without having technical background. Only the necessary cookies should be turned on by default. Most authorities in Europe share this opinion, but advertisement companies are fighting it. The previously mentioned EU ePrivacy Directive should provide future guidance. CCPA and data protection rules other than GDPR do not yet have a ruling such as this. Most of them only require information to be provided to the individuals, nothing more.

3.4 Cloud Computing

Cloud computing is now commonly used. ISO/IEC 19941:2017 (2017) states that cloud computing allows for network access to a scalable pool of physical or virtual resources that can be shared. Administration and self-service provisioning are also available.

Cloud computing consists of the following essential characteristics:

- Resource pooling: The cloud provider extracts resources and collects them into pools, then the portions of that pool are allocated to cloud customers.
- Broad network access: All resources are available via the internet.
- Rapid elasticity: Expanding and reducing the usage of cloud resources takes place as needed following demand patterns.
- Measured service: That which is provided by the cloud provider is metered. Charging is based on that measurement.
- On-demand self-service: Cloud customers manage the provisioning of resources on their own.

Cloud models come in different service models, the most common ones are listed below:

- Software as a service (SaaS) is a full application managed and hosted by the provider.
- Platform as a service (PaaS) is an IT platform that is provided, such as a database platform or several environments on which a customer can run their own application.
- Infrastructure as a service (IaaS) is a pool of fundamental IT services, such as servers with operating systems, network, or storage.

It should be noted that sometimes the lines between the different service models cannot be drawn accurately.

Finally, there are four different deployment models:

1. Public cloud: The cloud infrastructure is made available to the general public.
2. Private cloud: The cloud infrastructure is operated for one organization only.
3. Hybrid cloud: The cloud infrastructure is a composition of a public and private cloud.
4. Community cloud: Several organizations, usually from the same industry or geographic location, share cloud resources.

From a privacy perspective, the biggest challenge comes from the distributed nature of cloud resources. Cloud computing happens across the globe and it is often unclear where the resources of the cloud provider are really located. As a result, it can also be unclear where the data of an organization is currently located. Several data protection regulations require that PII is kept in the legislation or that special additional safeguards are implemented to allow the exportation of PII.

These challenges are usually addressed by the following means:

- The cloud provider offers options to restrict where the data is stored. Microsoft allows for the Azure cloud to define several regions and countries, and pricing is different for each region. Amazon also offers storage options like this as part of their Amazon Web Service (AWS) offerings.
- Cloud providers show the security of PII via certifications. ISO 27017 (Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services) provides security guidelines, whereas ISO 27018 (Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) is specifi-

cally tackling privacy. These certifications cannot circumvent the need for additional safeguards, such as model clauses, but can help to assure that certain standards are met.

- Model clauses or other contractual agreements are signed to ensure that exported PII is processed correctly.

The different legal obligations are challenging. Many countries require that organizations make data available to governmental agencies such as law enforcement agencies, national security agencies, and others. These requirements can directly conflict with privacy laws of the data-exporting countries. A way to mitigate this challenge is to understand and define where data are stored. Information can also be encrypted so a foreign law enforcement agency cannot access PII. However, keep in mind that the implementation of that cryptographic scheme needs to ensure that data at rest, in transit, and in use are encrypted in order to properly safeguard the information from a cloud provider seeking access.

The Cloud Security Alliance proposes 14 domains that should be investigated in order to achieve an adequate level of security (Cloud Security Alliance, 2017). These domains are summarized below:

1. Cloud computing concepts and architectures: This domain is the conceptual framework for the rest of the guidance. It describes and defines cloud computing, sets our baseline terminology, and details the overall logical and architectural frameworks used in the rest of the document.
2. Governance and enterprise risk management: This domain concerns the ability of an organization to govern and measure enterprise risk introduced by cloud computing.
3. Legal issues, contracts, and electronic discovery potential: This domain covers legal issues that may arise when using cloud computing. Issues covered in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.
4. Compliance and audit management: This domain addresses ways to maintain and prove compliance when using cloud computing.
5. Information governance: This domain focuses on governing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls that can be used to deal with the loss of physical control when moving data to the cloud, are discussed here.
6. Management plane and business continuity: This domain gives guidance on securing the management plane and administrative interfaces used when accessing the cloud, including both web consoles and APIs.
7. Infrastructure security: This domain covers core cloud infrastructure security including networking, workload security, and hybrid cloud considerations.
8. Virtualization and containers: This domain focuses on security for hypervisors, containers, and software defined networks.
9. Incident response: This domain gives guidance on proper and adequate incident detection, response, notification, and remediation.

10. Application security: This domain focuses on securing application software that is running on or being developed in the cloud. This includes reference to the OWASP top 10.
11. Data security and encryption: This domain addresses the implementation of data security and encryption and ensuring scalable key management.
12. Identity, entitlement, and access management: This domain covers managing identities and leveraging directory services to provide access control.
13. Security as a service: This domain focuses on providing third party-facilitated security services.
14. Related technologies: This domain addresses technologies with a relationship to cloud computing including big data, Internet of Things, and mobile computing.

SUMMARY

Implementing privacy is possible but requires certain techniques to be successful. Different variations of privacy provide different levels of privacy. More basic techniques, such as generalization and suppression, need to be considered and used carefully as individual data can still be revealed. Differential privacy provides a higher level of privacy assurance, but it always comes with the cost of making the data less usable. The right balance has to be found.

User tracking, cloud computing, and data science provide huge value for an organization, but each have certain challenges from a privacy perspective. Where user tracking is a topic of transparency and consent, data science brings us to an area where an organization has to find a balance between the interests of the organization and the individual. Purpose limitation and data minimization are in direct conflict with the needs of data science.

Cloud computing provides benefits, but it involves the data leaving the organization and essentially being processed somewhere else. Sometimes it is not easy to determine where and how the PII is processed and the cloud security alliance provides guidelines and a framework for explaining how to tackle it. In particular, cross-border transfers of PII are so easy that an organization has to consider the legality of them and agree to the contractual safeguards or data processing in a specific country or region.

UNIT 4

BUILDING BLOCKS OF CYBER SECURITY

STUDY GOALS

On completion of this unit, you will have learned …

- basic cyber security concepts and core cyber security buildings blocks.
- how to write a solid security plan.
- how to “secure” code and test Web applications in a security context.
- about the concept of DevSecOps.
- how to develop a secure IT system.
- how to best determine a cyber security framework for a company.

4. BUILDING BLOCKS OF CYBER SECURITY

Introduction

It is not simple to explain the concept and the necessary building blocks of cyber security without clarifying some basic concepts. Unlike information or IT security, the main objectives in cyber security are not only to defend digital information in the cyber world, but also to defend other vulnerable aspects of the information and communication technology environment. There are a lot of possible ways to define cyber security building blocks, but their main features include

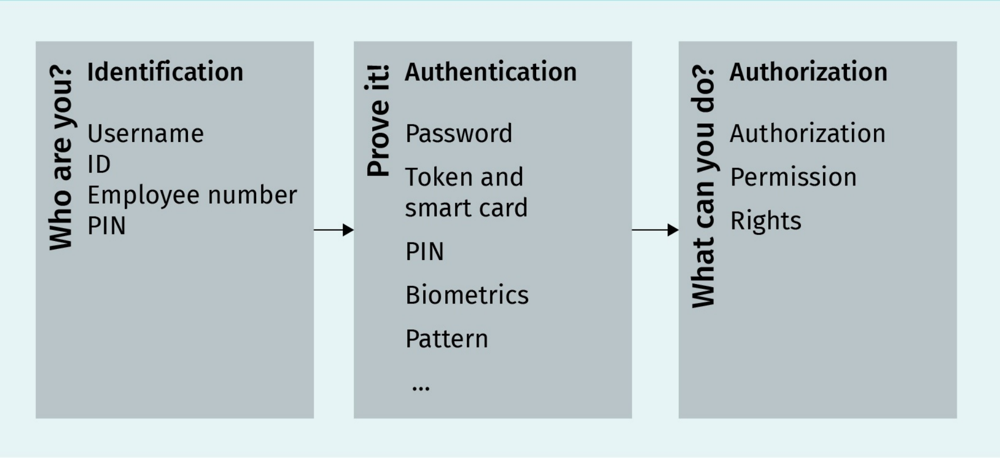
- identification, authentication, access management, accounting, and control (IAAA),
- network security,
- end-point security,
- information management,
- vulnerability, threat and incident management, and
- awareness, training, and education.

4.1 Authentication, Access Management, and Control

There are four basic concepts, known as IAAA (spoken “I triple A”), that must be known when managing access to a system. They are

- identification (who you are),
- authentication (proof of who you are),
- authorization (what you can do), and
- accountability (audit and audit logs concept).

Figure 5: Process of Gaining Access to a System



Source: Created on behalf of IU (2020).

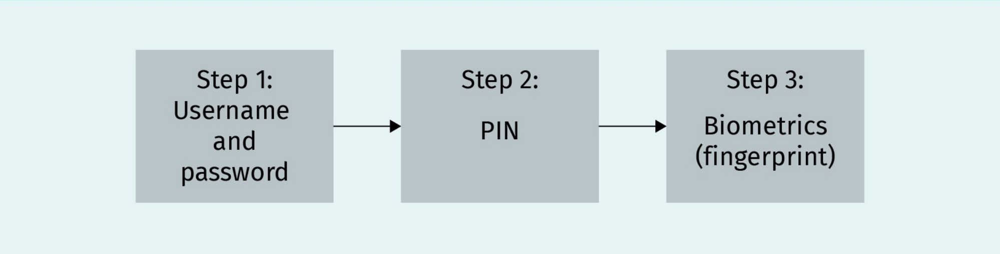
The figure above shows the steps that should be taken in order to gain access to a system. For the identification phase we need to have obtained one or more of the following: ID, username, employee number, PIN, or something similar from HR. In order to move through the authentication process, there is a requirement to produce something that we know (PIN, password, pattern, etc.), something that we have (token, smart card, etc.), or some biometric property (fingerprint, iris scan, etc.). After successful authentication, we will gain limited access to the resources (permission and rights). Authentication is designed to reduce the possibility that an unauthorized user obtains access by impersonating an authorized user. The organization's security policy should reflect how difficult it is for one user to impersonate another. Highly sensitive or valuable information demands stronger authentication technologies than less sensitive or valuable information (Pearson IT certification, 2002). The most common and least stringent form of authentication technology only demands that users provide a valid account name and a password in order to obtain access to a system or network. In environments where passwords provide the only barriers to entry and access, it is essential to understand how to create strong passwords and protect well-known accounts from attack. Today, most IT systems in companies already have a mechanism for checking password complexity known as the complexity rule. As of January 2020, common minimum requirements of the password policy dictate that passwords must be at least 12 characters long (a combination of uppercase and lowercase letters, numbers, and special characters), for example, "gnlemZUH70_$." The problem with such complexity is remembering this kind of password, but a user can build their own algorithm to help with remembering, or they can use third party software for password management. One risk of having weak passwords in computer-readable formats is that they can be used in a brute-force or dictionary attack. Effective authentication management is described in the new NIST Special Publication 800-63A-C—Digital Identity Guidelines (Grassi et al., 2019).

An alternative method for authentication is biometrics. Biometrics refers to metrics related to human characteristics. Biometric identifiers are measurable, distinctive characteristics that are used to label and describe individuals. By utilizing biometrics, a user could be distinguished by who they are instead of what they have (card, token) or what they know (secret key, PIN) (Kalyani, 2017). Biometric systems “read” some physical characteristic of the user such as a fingerprint, facial features, retinal pattern, voiceprint, hand geometry, or signature. Even the user’s way of walking or typing on a keyboard can be used as biometric authentication. These readings are compared to a database of authorized users, or a pattern, to determine identity. Authentication based on biometrics seems very secure at first sight, but experience shows some major drawbacks. First, there are several examples of overcoming such a system, for example using a fingerprint dummy based on a high-resolution photograph of a glass touched by the person concerned. Second, since different measurements of biometric properties of the same person are never identical, one must access a certain degree of deviation. If the deviation accepted is too large, this leads to a high false acceptance rate (FAR) where people with similar characteristics are accepted as well. If the deviation accepted is too low, this leads to high false rejection rate (FRR) where even legitimate users are not accepted and, if this happens repeatedly, may not be able to access the system. Third, while it is possible to change a password or PIN, it is not possible to change one’s biometric characteristics even if they have been “stolen” and are misused.

The next authentication method is security devices. These systems require the use of a special hardware device that functions like a customized key to gain system access. The device may be inserted into the system like a key or used to generate a code that is then entered into the system.

For enhanced security, two (2-Factor Authentication (2FA)) or more (Multi-Factor Authentication (MFA)) factors may be combined for authentication. This can be a username and password with other credentials, such as a code from the user’s smartphone or fingerprint, the answer to a security question, or facial recognition. The figure below shows a specific example of an MFA, or three factor combination of authentication (username and password + PIN + fingerprint).

Figure 6: Steps in the MFA Method

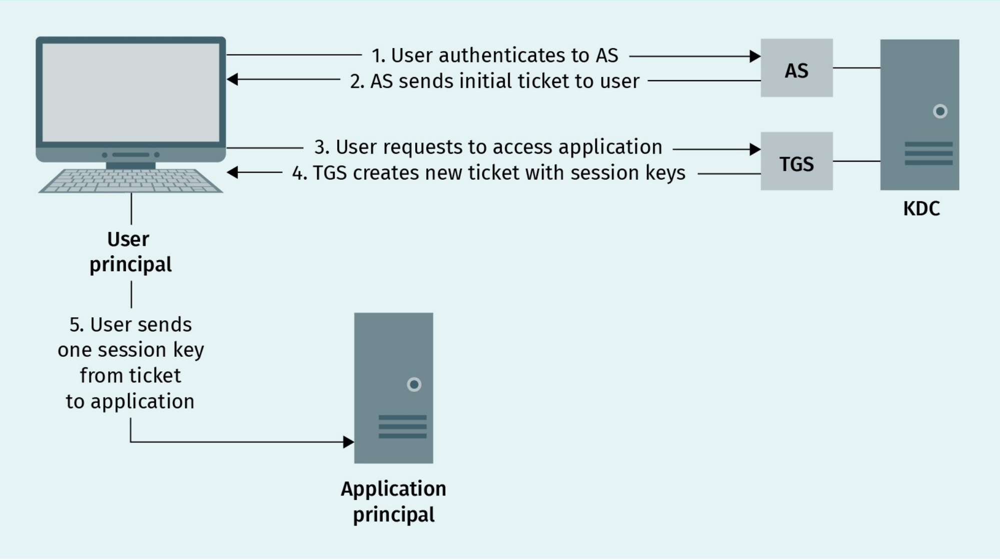

Step 1: Username and password
Step 2: PIN
Step 3: Biometrics (fingerprint)

Source: Created on behalf of IU (2020).

Single sign-on (SSO) is another method that many companies use. This is a combination of identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging in only once with just one set of credentials (username and password, for example). “SSO is the ability for a user to authenticate once to a single authentication authority and then access other protected resources without authenticating again. The Open Group defines SSO as the mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access permission, without the need to enter multiple passwords" (De Clercq, 2002, Abstract Section, para. 2).

Kerberos is a commonly used protocol for SSO in distributed environments. Kerberos is implemented in open source products but also in Microsoft Active Directory. The main component is a key distribution center (KDC) that holds the secret keys of all users and services. It provides an authentication service (AS) and a key distribution functionality. The KDC provides security services to the principals, which can be users, applications, or other network services. The KDC must have an account for every principal. A ticket is generated by the ticket granting service (TGS) on the KDC and given to a principal. The ticket enables the principal to authenticate to another principal (Neumann et al., 2005).

Figure 7: Kerberos, a Common SSO Protocol, Authentication


1. User authenticates to AS
2. AS sends initial ticket to user
AS
3. User requests to access application
4. TGS creates new ticket with session keys
TGS
KDC
User principal
5. User sends one session key from ticket to application
Application principal

Source: Created on behalf of IU (2020).

There are two methods of access—physical and logical. Physical access control is a mechanical form—for example physical access to a room (locker server room) with keys. Physical access can be achieved with physical keys, or it can be controlled by an application or system software with a chip on an access card.

Logical access controls tools that are used for credentials, validation, authorization, and accountability in cyber infrastructure and the systems within it. These components are often implemented on several levels and enforce access control measures for systems, applications, processes, and information. This type of access control can also be embedded inside an application, operating system, database, or administrative system (Vacca, 2014).

Today, there are numerous methods of access controls implemented in real-world settings. These include the following:

- Mandatory Access Control (MAC),
- Discretionary Access Control (DAC),
- Rule-Based Access Control, and
- Role-Based Access Control (RBAC).

In a Mandatory Access Control (MAC) environment, all requests for access to resources are automatically subject to access controls. In such environments, all users and resources are classified and receive one or more security labels (such as “Unclassified,” “Secret,” and “Top Secret”). A well-known form of MAC is the Bell-LaPadula model where a user can only access a resource if the user’s security label is at least as high as that of the resource. Any resource created or written by a user automatically receives the security label of the user. This approach works well for protecting confidentiality (no read-up) but, in its pure form, makes it impossible for a user to communicate to other users who have a lower security label (no write-down). The Biba model, on the other hand, puts the emphasis on integrity rather than on confidentiality of the resources, therefore defining that a user can only access a resource if the user’s security label is as high as that of the resource (no read-down, no write-up). Since this leads to similar problems as Bell-LaPadula, both models are useful as a basis but rarely used in pure form, only in weakened forms. For example, in the Biba model, users are additionally allowed to access resources with lower security levels, but only after they have explicitly confirmed that they want to access such less trusted data.

In a Discretionary Access Controlled (DAC) environment, resource owners and administrators jointly control access to resources. This model allows for much greater flexibility and drastically reduces the administrative burdens of security implementation. In general, rule-based access control systems associate explicit access controls with specific system resources, such as files or printers. In such environments, administrators typically establish access rules on a per-resource basis, and the underlying operating system or directory service employs those rules to grant or deny access to users who request it. Rule-based access controls may use a MAC or DAC scheme, depending on the management role of the resource owners. Role-based access control (RBAC) enforces access controls depending on a user’s role(s). Roles represent specific organizational duties and are commonly mapped to job titles such as “A/P clerk,” “receptionist,” or “chief executive officer.” Obviously, these roles require vastly different network access privileges (Chapple et al., 2002).

Considering that users need access to a large number of applications, websites, Web services, etc., it is important to have a “simple” method of authentication without a lot of complex passwords or cards with chips. One solution to this challenge was offered by the FIDO Alliance. The FIDO2 specifications are the World Wide Web Consortium’s (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance’s corresponding Client-to-Authenticator Protocol (CTAP) (FIDO, n.d.). The idea to have sound authentication methods without passwords and/or complex hardware has been implemented through “passwordless” authentication, two-factor authentication, or multi-factor authentication in combination with biometrics. All of these options can be implemented in a simple piece of hardware.

The FIDO alliance proposes a simpler and more effective standard regarding authentication. It specifically addresses the challenges around the dependency on passwords (FIDO Alliance, n.d.-b). FIDO2 is comprised of the W3C Web Authentication specification and corresponding Client-to-Authenticator Protocols (CTAP) from the FIDO Alliance. FIDO2 supports passwordless, second factor, and multi-factor user experiences with embedded (bound) authenticators such as biometrics or PINs, or external (roaming) authenticators such as FIDO Security Keys, mobile devices, wearables, etc. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services. Biometric information, if used, never leaves the user's device (mobile phone, USB stick, PC, etc.) (FIDO Alliance, n.d.-a).

Auditing capabilities ensure that users are accountable for their actions. They can be used to verify users' actions and help during investigations. Audit documentation and log files hold a massive amount of information and the challenge is often to reduce it to the relevant parts. Audit trails contain information about operating system activity, application events, network events, and user actions. Audit trails can also be used to alert system administrators or managers of a certain event. They can also be used later for forensics during a criminal investigation. Audit trails can be reviewed manually or automatically, but they must be reviewed and analyzed. A Security Information and Event Management (SIEM) system can help to manage audit trails and alerts (Nieles et al., 2017). On the other hand, audit trails create new challenges since they collect the personal data of the users, so an adequate compromise must be found for any specific system.

4.2 Endpoint Security

General concept endpoint security refers to securing "end-user devices" like desktops, laptops, and mobile devices. Conversely, servers in datacenters can also be considered endpoint devices. It is very hard to give a precise definition, but in the context of cyber security, it can be said that endpoint devices are users' devices that are connected to the network. Endpoint security does not only involve antivirus-software protection. Endpoints serve as points of access to an enterprise network and create points of entry that can be exploited by malicious actors. Therefore, many types of endpoint protection are needed, including antivirus-solutions, Internet of Things (IoT) security, network access control, detection and response, encryption, and sandboxing to name just a few. There are many features that endpoint security may have, such as

- data loss prevention (DLP),
- protection against insider threat,
- endpoint detection and response,
- encryption (email, communication, full disk),
- application whitelisting or control,
- network access control (NAC),
- data classification, and
- privileged user control.

Sometimes, the protection of endpoint devices is included in third party software; however, it can also be included in the development of the hardware itself, or the “security by design” concept. This building block of cyber security must be taken seriously in the process of developing a cyber security program or strategy. Below, the combination of featured endpoints will be explained.

The simplest way to explain endpoint security in action is through the protection of PCs or laptops—the most-used endpoint devices in corporate settings. When securing these devices, we are not only securing the data stored on these devices, but also the entire corporate network. This means that many features must be implemented in order to achieve this level of security.

When securing data and preventing data loss (data loss prevention or DLP), we first need to prioritize, categorize (classify), and label information because not all information has the same level of sensitivity. This is done through an internal company procedure, for example, according to ISO27001, Annex A.8.2.1 and A.8.2.2. Typical classification levels in the public sector are public, internal, secret, and top secret. In the private sector, public, internal, restricted, and private are often used. After that, risk needs to be managed and a procedure for monitoring the movement of data needs to be established. Typically, there is always some kind of “.log” file monitoring system, such as SIEM (Security Information and Event Management System). Logging data flow is very important in this process, as the only way to get adequate information about security incidents that arise, or have already occurred, is through data analysis. Protection from an external threat, such as malware and malicious activity, is just as important and should always be part of corporate policy, including local anti-virus protections, centralized monitoring, and anti-virus management. Firewall protection is very often combined with this kind of software in order to protect access to and from external resources. Network security and privacy is not only implemented through firewalls and rules, but also through encryption, proxy, and VPNs. In a situation where we want to defend and protect our data and information on our end devices or the flow of our data across the network, we will use cryptography and encryption features. This can be a partial encryption of “top-secret” classified data, encryption of the whole disk (a very common situation), or encryption of data flow across the network with a VPN.

4.3 Cyber Security in Networks

Network security focuses on the security of communication networks.

Network security consists of policies, procedures, and practices which are adopted to monitor, prevent, and defend against unauthorized access, misuse, modification, or denial of service. Network security covers a variety of computer networks—public and private, LAN, WAN, and others that are used in everyday jobs. Networks can be private company networks or open to public access.

Cyber security in networks consists of protection, detection, and reaction phases. “Protection” means that systems and networks must be configured as correctly as possible with implemented security measures. “Detection” identifies when the configuration has changed or when some network traffic indicates a problem. “Reaction” is the response to a problem and the return to a safe state as quickly as possible. Today, most cyber security frameworks, such as NIST and CSF, recommend working with these phases.

Cyber security
In networks, cyber security consists of the protection, detection, and reaction phases, although identify and recover phases can also be found in some cyber security frameworks.

There are many proposed methods and techniques, including the following:

- Access control blocks unauthorized users and devices from accessing the network. Users that are allowed network access should only be able to work with the limited set of resources for which they have been authorized (need to know/need to access principle).
- DLP (data loss prevention) implements processes to ensure that data is not exfiltrated out of the network.
- Firewalls follow the rules that are defined to permit or deny network traffic between the network and the internet (militarized and de-militarized zone). They establish a barrier between trusted and untrusted sites.
- The intrusion detection and prevention system (IDS/IPS) scans network traffic to identify and block attacks, often by correlating network activity signatures with databases of known attack techniques.
- Network segmentation—Network and software-defined segmentation puts network traffic into different classifications and makes it easier to enforce security policies.
- Security information and event management (SIEM) products aim to automatically pull together information from a variety of network tools to provide the data you need in order to identify and respond to threats.
- Virtual private networks (VPN) are systems (typically based on IPsec or SSL) that protect the communication between a device and a secure network, creating a secure, encrypted “tunnel” across the open internet.
- Web security controls internal staff’s Web use in order to prevent Web-based threats from using browsers as a vector to infect your network (Fruhlinger, 2018).

Incident management includes proactive and reactive processes so that incidents can be detected and then dealt with. A SIEM system often helps, and a security operations center (SOC) handles the incident. The team that consists of several (IT) experts to handle a concrete incident is a computer emergency response team (CERT). There are many incident models and processes available that typically follow this structure:

1. Detection: An organization must realize that an actual incident has taken place, e.g., an attack. Sensors and SIEM systems help to detect an incident.
2. Response: The next step is to determine what the actual response will be. Usually more data is gathered and analyzed at this stage to respond adequately. It is not good to blindly change IPS or firewall rules at this point in time but to first understand what an attacker wants, who they are, and what methods are used.
3. Mitigation: The next step is to mitigate or contain the damage caused by the incident. The goal is to prevent or reduce further damage from this incident. Mitigation happens based on priority, so information of a high value (e.g., sensitive PII) will be contained and protected first.

4. Reporting: Incident reporting and documentation happens throughout the process. Often, someone else reports the unusual behavior of a system, then the CERT team gets involved. Documenting the incident also plays a role in legal disputes or when deciding whether a cyber security insurance needs to get involved afterwards.
5. Recover: Once the incident is mitigated, all systems and information must be enabled again. Before that, evidence must be gathered for further forensics. This phase includes fixing what was broken by the incident.
6. Remediation: In the last phase of an incident, it is ensured that the attack cannot be successful again. In this phase, it is decided which measures are implemented, such as firewall settings. Learning what went wrong and what can be done better is also an important action in this phase.

Authentication, authorization, and accounting are important requirements during a remote access session (RAS).

A central authentication service for dial-up users is the standard remote authentication and dial-in user service (RADIUS). RADIUS incorporates an authentication server and dynamic passwords. The RADIUS protocol is an open, lightweight, UDP-based protocol, and the program can be modified so that it can work with a lot of security systems. It provides authentication, authorization, and accounting services to routers, modem servers, and wireless applications. RADIUS is described in RFC 2865. The NAS also provides accounting information to the RADIUS server for documentation purposes (Cole et al., 2005). An updated and improved version of the RADIUS protocol was published as DIAMETER protocol.

Terminal access controller access control system (TACACS) is an authentication protocol. TACACS provides remote access authentication and related services (event logging).

Another authentication mechanism is the password authentication protocol (PAP). In PAP, a user provides an unencrypted username and password. Those are compared with the corresponding information stored in a database of authorized users (patterns). The challenge handshake authentication protocol (CHAP) is described in detail in the RFC 1994 standard, but in short, provides authentication after the establishment of the initial communication link between the user and CHAP (Cole et al., 2005).

Yet another method of remote authentication is callback. In callback, a remote user dials in to the authentication server, provides an ID and password, and then hangs up. The authentication server looks up the caller’s ID in a database of authorized users and obtains a phone number at a fixed location. The authentication server calls the phone number, the user answers, and then the user has access to the system (Cole et al., 2005).

Extensible authentication protocol (EAP) is extension of point to point and is described in IEEE 802.1x. Its main task is to secure a connection with point to point or access to the network, which is only possible after authentication.

4.4 Developing Secure IT Systems

The first prerequisite for a secure IT system is a **cyber security plan**. This plan is always part of a cyber security strategy, which must be compatible with the corporate strategy. In this section, we will describe **Common Criteria** (CC) and evaluation assurance level, which are the technical base for product security evaluation and certification. At the end of this section, two examples of good practices will be presented—Open Web Application Security Project (OWASP) and development security operation (DevSecOps).

Cyber security plan
A cyber security plan must be incorporated in to the cyber security and corporate strategies.

Common Criteria
This can be used as a guide or template for the development of cyber security systems.

> The Common Criteria for Information Technology Security Evaluation (CC), is technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that
>
> - products can be evaluated by competent and independent licensed laboratories to determine the fulfilment of particular security properties to a certain extent or assurance.
> - supporting documents are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.
> - the certification of the security properties of an evaluated product can be issued by several Certificate Authorizing Schemes, with this certification being based on the result of their evaluation.
> - these certificates are recognized by all the signatories of the CCRA (Common Criteria, n.d., The Common Criteria Section, para. 1).

The CC can be used as a guide for the development, evaluation, and/or procurement of IT products with security functionality. CC is described in ISO standard ISO/IEC 15408. The basic terms used in the CC domain are explained below.

- Target of evaluation (TOE)—the product or system that is the subject of the evaluation, which also has the following security features:
  - Protection profile (PP)—a document which describes security requirements, for example, for equipment.
  - Security targets (ST)—a document that identifies the security properties of the target of evaluation.
  - Security functional requirements (SFRs)—these specify individual security functions which may be provided by a product.

Quality of the product can be achieved by paying attention to the following:

- Security assurance requirements (SARs) are measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.
- Evaluation assurance level (EAL) is the numerical rating describing the depth and rigor of an evaluation (Common Criteria, 2017). Common Criteria lists seven levels of EAL with EAL 1 being the most basic and EAL 7 being the most stringent:
  - EAL1—functionally tested
  - EAL2—structurally tested
  - EAL3—methodically tested and checked
  - EAL4—methodically designed, tested, and reviewed
  - EAL5—semi-formally designed and tested

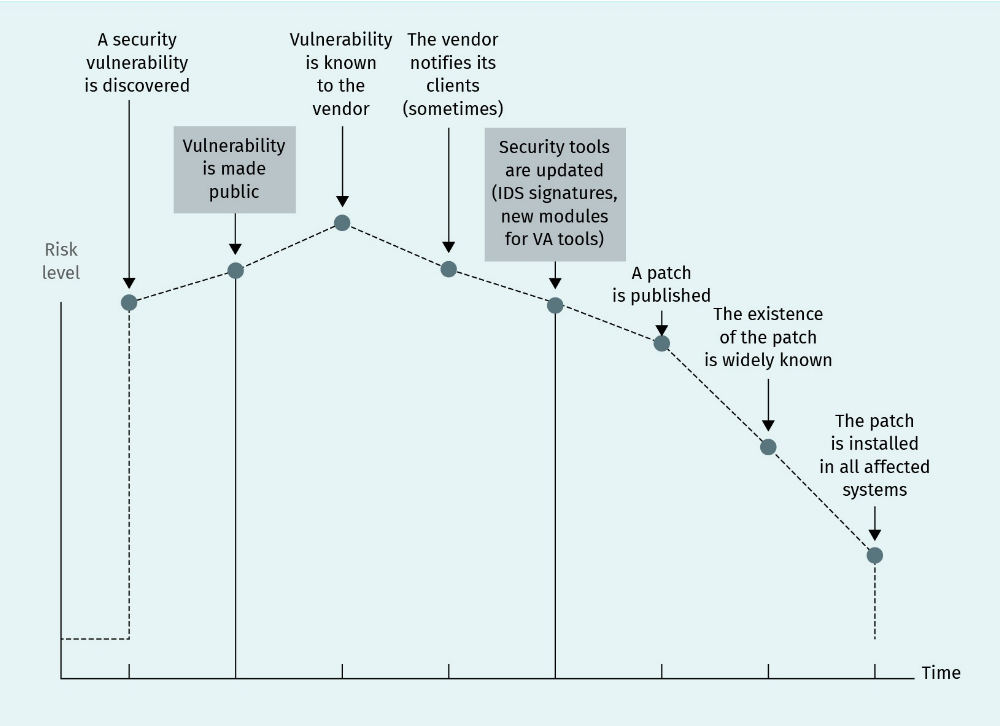
- EAL6—semi-formally verified design and tested
- EAL7—formally verified design and tested

A higher EAL does not necessarily mean that the products are more secure, but rather that more thorough verification was performed. To better understand CC certification, the following are examples of some steps that companies must take to become CC certified:

- Security target (ST) and other supporting documents, such as an overview of the products with emphasis on security features and potential security threats, must be complete.
- Self-assessment with documentation regarding the way that products conform to the structure of protection profile and evaluation assurance level test must be completed.
- Evaluation of the products must be completed in an independent licensed laboratory. There must be proof that the products' security level is at a "satisfactory level."
- If the security level of the product is satisfactory and the product passes the evaluation, certification will be given by various certificate authorizing schemes (CAS).

A good way to build a secure IT system is to use the OWASP Security Knowledge Framework. It can be used as a guide to help with the building and verification of secure software. In the secure software development life cycle, education is the first step, so this framework is useful when training developers in the area of application security.

Figure 8: High Level View on Vulnerability Concept


A security vulnerability is discovered
Vulnerability is made public
Vulnerability is known to the vendor
The vendor notifies its clients (sometimes)
Security tools are updated (IDS signatures, new modules for VA tools)
A patch is published
The existence of the patch is widely known
The patch is installed in all affected systems
Risk level
Time

Source: Open Web Application Security Project, 2017.

The source code of an application must be good and secure, but what is good and secure source code? One of the organizations that produces good coding standards is Carnegie Mellon University's Software Engineering Institute (SEI). SEI's top ten secure coding practices are as follows (Seacord, 2018):

1. validate input. Validate input from all untrusted data sources.
2. heed compiler warnings. Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code.
3. create architecture and design for security policies. Create a software architecture and design your software to implement and enforce security policies.
4. keep it simple. Keep the design as simple and small as possible.
5. deny by default. Base access decisions on permission rather than exclusion.
6. adhere to the principle of least privilege. Every process should execute with the least set of privileges necessary to complete the job.
7. sanitize data sent to other systems. Sanitize all data passed to complex subsystems. The calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.
8. practice defense in depth. Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can prevent a security flaw from becoming an exploitable vulnerability and/or limit the consequences of a successful exploit.
9. use effective quality assurance techniques. Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should all be incorporated as part of an effective quality assurance program.
10. adopt a secure coding standard. Develop and/or apply a secure coding standard for your target development language and platform.

The SEI publishes secure coding practises for many programming languages, including Java, C, and C++. Another good approach that helps to "make everyone responsible for security" is DevSecOps—an extension of the well-known concept DevOps. Successful security programs involve three intersecting parts: people, processes, and technologies. DevSecOps is no different, but it recognizes that security is the responsibility of everyone in an organization, and that everyone has a role to play in security. This means that people are the main priority in DevSecOps implementation. Hiring security specialists and experts, giving them a voice in project delivery, and allowing them to integrate their processes in the agile development world will deliver the necessary results. Agile development helps to speed up product release dates, but often at the cost of neglecting security. Appointing people to be in charge of security and providing good training will also ensure that security is a priority in an organization. Despite people being the main focus, processes are also key to the success of DevSecOps. Version control, metadata, orchestration, integration, compliance, security architecture, incident management, and threat intelligence are just some of the main processes in DevSecOps implementation. The end goal is to have technologies that enable people to properly execute DevSecOps processes (Raynaud, 2017).

Control A14.2 in ISO27001 Standard about security in development and support processes has the objective of ensuring that information security is designed and implemented within the development life cycle of information systems. The requirements are described in

- A.14.2.1 Secure Development Policy,
- A.14.2.2 System Change Control Procedures,
- A.14.2.3 Technical Review of Applications After Operating Platform Changes,
- A.14.2.4 Restrictions on Changes to Software Packages,
- A.14.2.5 Secure System Engineering Principles,
- A.14.2.6 Secure Development Environment,
- A.14.2.7 Outsourced Development,
- A.14.2.8 System Security Testing, and
- A.14.2.9 System Acceptance Testing.

Additionally, there are requirements in IEC/IAS 62443-4-1 ("Secure product development life cycle requirements"). This Standard describes security management, development process, and all security requirements in the life cycle of IT/OT products in industry.

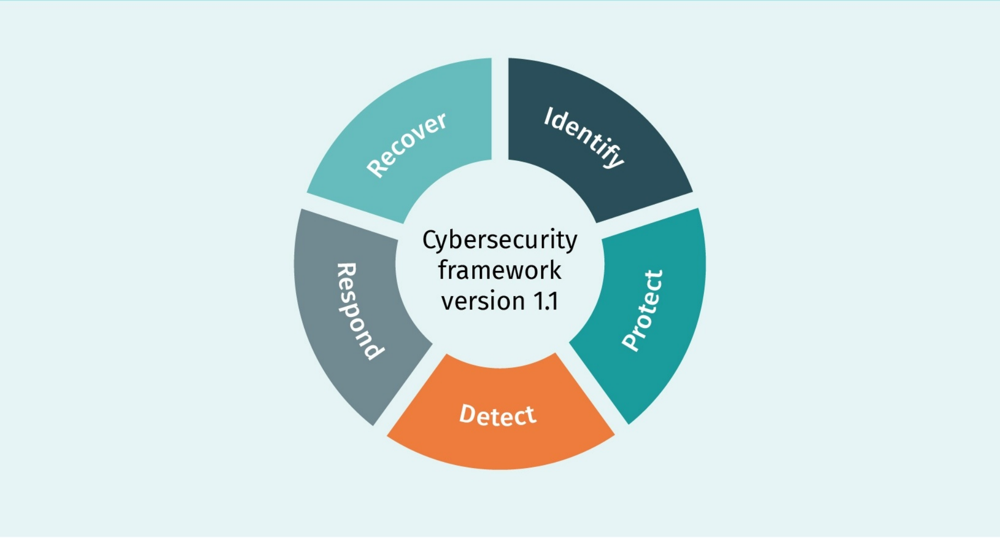
A prerequisite for a secure IT system is a security framework. We will now discuss the most important and most used cyber security frameworks—NIST CSF, ISO27K, NIST 800-53, and IEC 62443.

Today's cyber security models have evolved from models of computer security from a time when IT existed in the form of standalone computers, possibly connected in a local area network, without the internet, cyber space, or today's services and technologies. Computer security models offered a scheme for the specification and implementation of security policies and were, in fact, formal descriptions of security policies.

The Cybersecurity Framework is a product of NIST (National Institute of Standards and Technology USA) and, as of April 2018, the current version is 1.1. The framework is a risk-based approach, and it has the following three components:

- Core is a framework made up of a set of cyber security activities, desired results, and applicable references that are common to critical infrastructure sectors. The box itself consists of five competitive and constant functions—identify, protect, detect, response, and recover.
- Framework implementation tier(s) provide content and a way for an organization to approach and act in order to manage the risk.
- Framework profiles, in fact, represent results based on business needs, selected by the organization within the framework itself (National Institute of Standards and Technology, 2018).

Figure 9: NIST Cybersecurity Framework



Source: National Institute for Standards and Technology, 2018.

A practically applicable characteristic of the framework itself is that it offers a complete list of functions, categories, subcategories, and informative references that describe specific cyber security activities, which are most common in all critical infrastructure sectors. NIST (National Institute of Standards and Technology) released publication 800-53 as part of a special series of NIST-800 publications consisting of a catalogue of 20 security and privacy control groups. Control groups are conceived and implemented as very flexible and adaptable to users or organizers of different profiles. They are most often used as controls for risk management strategies. The areas covered by the controls are access control, security awareness, risk assessment, incident response, and monitoring (National Institute of Standards and Technology, 2020).

CIS Critical Security Controls is a product developed by the SANS institute that aims to publish a set of actions/activities for cyber defense. The document lists 20 controls, prioritized as hardware, software, configuration, malware defense, data recovery, account monitoring, incident response, pen-test, and red-team training (Center for Internet Security, n.d.). The “Information Security Standard” is essentially a two-part standard, the first of which is ISO27001. It provides the ISMS (Information Security Management System) specification with Annex A (a checklist), while the second part is ISO27002 “Code of Practice,” which is essentially a guide consisting of the best information security practices from around the world. ISO27001 and ISO27002 are connected because if organizations use Annex A controls, ISO27002 will offer them a way to implement those controls (International Organization for Standardization, 2019).

The IEC 62443 series of standards have been developed by the ISA99 committee (Industrial Standard for Automation) and the IEC (International Electrotechnical Commission), with the aim of highlighting the need to design a cyber security framework for the Industrial Automation Control System (IACS). The goal of applying this series of standards is to improve the security, availability, confidentiality, and integrity of the system components, as well as the system as a whole. Requirements of the standard itself are not only to improve electronic security, but also to identify and point out vulnerabilities while minimizing the risk of compromising information, confidentiality, or causing degradation or failure of controlled equipment (hardware or software). The set of standards was conceived and implemented for **ICS, SCADA**, and IACS systems (industry) and consists of 13 standards divided into groups as follows:

ICS, SCADA
Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems steer and control industrial IT, such as manufacturing equipment or power plants.

- General (62443-1-1, 62443-1-2, 62443-1-3, 62443-1-4)
- Policies and procedures (62443-2-1, 62443-2-2, 62443-2-3, 62443-2-4)
- System (62443-3-1, 62443-3-2, 62443-3-3)
- Component (62443-4-1, 62443-4-2)

As explained, there are many different approaches when selecting models and frameworks for cyber security; however, the generalization and the uniform approach to selecting the right model or framework is questionable. Cyber security is needed by small businesses, organizations, medium and large businesses, large corporations, administrations, industries, civil society, and universities—each of these has its own specificities. They could have different requirements for the size, domain, and sphere of business, activity, service provided, and products produced. This imposes the need for a tailored approach when selecting a framework or cyber security model (DKE VDE, 2019).

SUMMARY

It is not so simple to talk about cyber security building blocks, as there are many concepts and approaches when dealing with cyber security. In this unit, we explained how to choose the most important concepts in the cyber security domain and how to recognize essential building blocks.

When choosing an appropriate cyber security framework, it is very important to know what kind of company or organization it is being chosen for. Sometimes we can use just the ISO27K framework, but sometimes the IEC62443 framework is required. In some situations, it is necessary to combine NIST CSF, IEC62443, and ISO27K.

When building a cyber security system, we must employ an experienced team consisting of experts in cyber security. This unit also recommends the use of OWASP and DevSecOps concepts when building cyber security systems.

UNIT 5

IT SECURITY MANAGEMENT

STUDY GOALS

On completion of this unit, you will have learned …

- how to manage cyber security holistically.
- what role the security policy plays.
- how to use risk management to steer and control cyber security.
- how IT security and IT governance collaborate.
- what the PCI DSS standard is and how it implements security management.

5. IT SECURITY MANAGEMENT

Introduction

Cyber security is not only an important practice within an organization, but it also plays a crucial role when managing an enterprise in current times. As organizations become completely dependent on the confidentiality, integrity, and availability of the information they handle, the need to manage security has continued to increase, even for industries not directly related to IT. It is important to understand the business priorities to make sure that security incidents do not threaten the critical systems of an organization. The tools, processes, and controls needed to protect an organization's assets are as complex as the information systems they are designed to protect.

When combined, business objectives, a strategy, security policy, priorities, standards, processes, controls, and metrics help to foster a holistic cyber security management program. This is also known as an Information Security Management System (ISMS).

Further risk management helps to identify and evaluate potential negative outcomes in relation to the CIA triad of cyber security.

5.1 Security Policy

The development of a security policy is a foundational component in any security management system. The policy defines the principles and actions that are required so that the organization can protect its assets and personnel. The main audience for a security policy is the personnel of an organization. Hence, it must be easily accessible and readable so that the lack of expert knowledge is not an excuse for policy violations. Many organizations require their personnel to acknowledge the security policy formally, both initially and during an annual process. Different parts of the policy can address different audiences. So, IT engineers can be addressed via more technically specific policy statements than other individual contributors in an organization. To be effective, communication of the policy needs to follow organizational practices and can be supported by video recordings and mentioning it at regular meetings, for example. It is important that executive management leads by example and acts in compliance with the policy; otherwise, a policy can easily become ineffective. The security policy must be aligned with applicable laws, regulations, standards, and contractual obligations. Privacy should be considered, and it must fit into the organizational culture.

Controls

A security policy must be aligned with controls. Controls are formal descriptions, safeguards, or counter measures used to detect, avoid, counteract, or minimize risk towards the information assets of the organization. Controls can be classified as preventative, detective, or deterrent.

- Preventative controls: These controls prevent the occurrence of an unwanted event. Examples are badge entry systems or login screen messages that prevent unauthorized people from entering a building or accessing an IT system.
- Detective controls: These controls record both good and bad events. Video surveillance or event logs of a server are examples of a detective control.
- Deterrent controls: These controls convince somebody not to act in a certain way. Examples are warning signs or watch dogs. Video surveillance systems also act as a deterrent, as they are detective controls.

Three types of controls that exist are as follows:

1. Physical. These controls exist in the physical world and include video surveillance, locks on doors, and fences.
2. Technical. These controls are implemented in IT systems, and some examples are access control lists, audit logs, and encryption mechanisms.
3. Administrative (sometimes referred to as managerial controls). These controls are protocols, processes, standards, and policies that forbid or require a certain activity. Examples are rules that only allow certain software installations on a device or forbid the connection of private devices to the network.

The security policy must be in alignment with the controls. For every policy statement, a control must exist and vice versa, but they must not contradict each other.

Security Policy Structure

Security policies can be structured in many ways. Whether the policy consists of one document or several different documents with references to each other is the choice of the organization. Generally, it should align with the way that other policies are published. A security policy statement should be general in nature and should not cite specific devices, technologies, or configurations. It should state what needs to be done, not how it needs to be done. That way, the statement does not need to change as often. Various topics are included, such as the following:

- Acceptable use
- Anti-Virus / malware
- Mobile device
- Password
- Bring your own device (BYOD)
- Email and communications
- Social media
- Physical security
- Cloud security
- Security incidents
- Third party security

5.2 Security and Risk Analysis

Cyber security risk management is the practice of balancing business opportunities with potential cyber security-related negative outcomes. It is largely a qualitative effort, since it is difficult to know the probability and impact of potential negative outcome events. In this section, several quantitative metrics will be presented, as they have been established to measure and better understand how to handle risk.

Threats, Vulnerabilities, and Risk

The following terms are often misunderstood and need to be defined clearly in order to understand risk.

- Asset: An asset is what needs to be protected, for example, information, people, or property.
- Vulnerability: A vulnerability is a weakness or gap in the protection of an asset that can be exploited by threats to impair the CIA of the asset.
- Threat: A threat is anything that can exploit a vulnerability. It damages, obtains, or destroys an asset, whether intentionally or accidentally.
- Risk: A risk is the intersection of an asset, a threat, and a vulnerability. It can be written as $\text{Risk} = \text{Asset} + \text{Threat} + \text{Vulnerability}$. A different, more general definition describes a risk as a potential damage that has a certain impact and a certain probability of occurring.

For example, a Windows server (the asset) does not have the latest patch installed. This is a vulnerability. A hacker (threat actor) can try to exploit this vulnerability to gain access to the customer database stored on that server. This is the threat. The risk is the combination of an unpatched server with a missing patch that can be exploited by a hacker.

Microsoft proposes the STRIDE model to categorize threats. STRIDE stands for

- Spoofing identity
- Tampering with data
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege (Microsoft, 2009)

The DREAD risk assessment model was originally created to categorize threats, as well as risks. The creator, Microsoft, no longer uses it.

Dread stands for

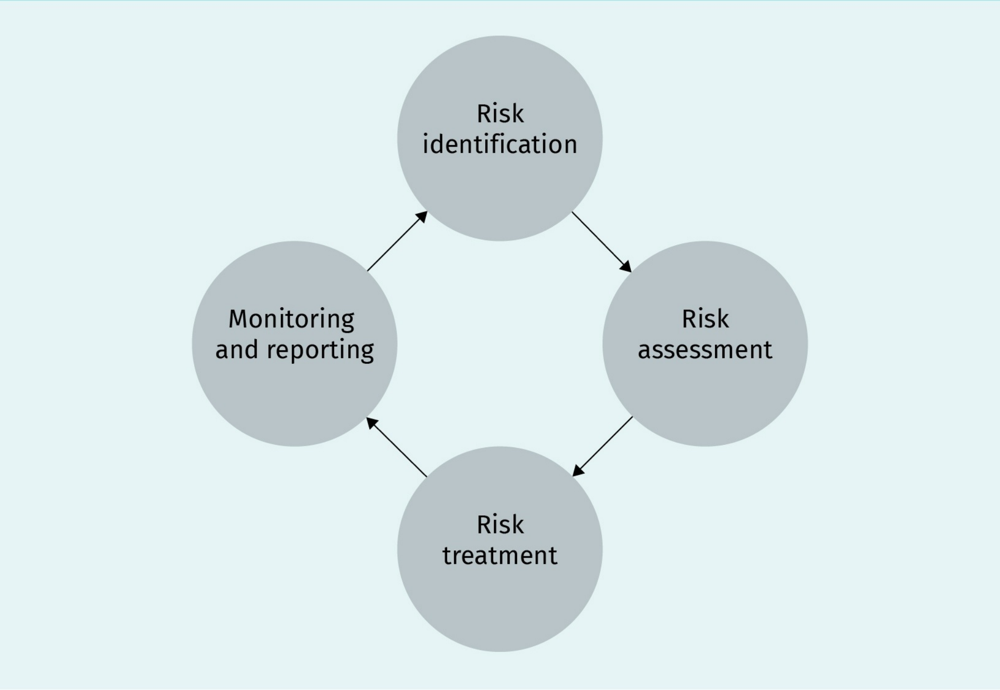
- damage (How bad would an attack be?),
- Reproducibility (How easy is it to reproduce the attack?),
- Exploitability (How much work is it to launch the attack?),
- Affected (How many people will be impacted?), and

- Discoverability (How easy is it to discover the threat?) (OpenStack, n.d.).

The OWASP top ten vulnerabilities are a good example of typical vulnerabilities in Web applications.

Risk Management Process

Figure 10: A Risk Management Process



Source: Created on behalf of IU (2020).

The figure above shows a typical risk management process. In the risk program, an organization defines the scope of the risk management activities. It typically includes the businesses and geographical areas that are in scope, as well as other parameters. During this phase, an organization also defines its risk appetite or risk tolerance. It expresses the level of risk that an organization is willing to take. In most organizations, this is described in qualitative terms; however, in the financial industry (banks, insurances, etc.), we sometimes find quantitative terms. Note that a risk-free business does not exist, and risk is an integral part of business and life, so it is not necessarily negative.

Risk identification is the first step in the iterative risk management process. The organization identifies risks, vulnerabilities, and threats. Risk assessment is the second step in the iterative approach, and several characteristics are determined. These are the probability that the risk occurs, the impact the risk event would have, any available risk mitigations, and a recommendation of how to address the risk. Risk treatment is typically the last step of the risk management process. A decision-maker or a risk committee decides how to treat each specific risk. There are four options for risk treatment.

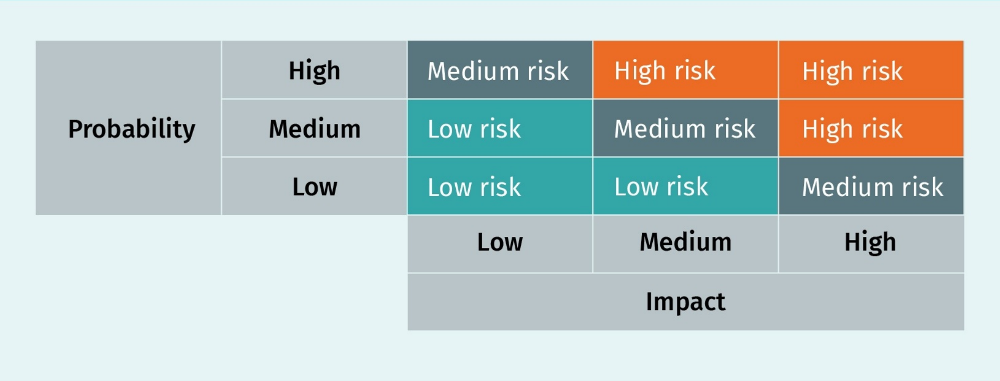
1. Accept: The organization decides not to take any action regarding the risk.
2. Mitigate: Some actions are taken to reduce impact, probability, or both to an acceptable level.
3. Transfer: A risk is transferred to a third party, usually an insurance company. Other forms are available, for example, specific contractual agreements with third party suppliers.
4. Avoid: The organization chooses to end the activity associated with the risk. This is often the option when business activities are not needed any more or outdated systems are turned off.

Note that risk ignorance is not a valid risk treatment option.

Qualitative and Quantitative Risk Management

In qualitative risk analysis, the probability and impact of an event can be expressed on a scale labeled high, medium, and low. The scale does not identify the exact value but usually has a description of what the different levels mean. It can be used to quickly understand risks in relation to each other. The figure below shows a typical qualitative risk matrix.

Figure 11: Qualitative Risk Matrix



Probability	**High**	Medium risk	High risk	High risk
	Medium	Low risk	Medium risk	High risk
	Low	Low risk	Low risk	Medium risk
		Low	**Medium**	**High**
		Impact		

Source: Created on behalf of IU (2020).

Using an odd number of levels often makes risks lean towards the middle, hence an even number of levels is often chosen.

Sometimes, semi-quantitative methods are chosen. This can be achieved by assigning numbers to the different levels, such as 1 to low and 3 to high. Then, the numbers are multiplied to provide a risk level such as: $\text{high probability} \cdot \text{medium impact} = 3 \cdot 2 = 6$. So the risk level would be 6 in this example. Here, the different values only determine the risk level in relation to each other.

In quantitative risk analysis, the actual costs and the probability of events are determined. Achieving the accuracy needed in order to come up with the exact event probability for every scenario is difficult, if not impossible. Also, the exact costs of an event are difficult to determine as incidents are often complex, and short- and long-term outcomes are not easy to predict. Because of these challenges, quantitative risk analysis should try to develop estimates, such as ranges, rather than exact figures.

Several figures can help when carrying out quantitative risk analysis.

1. Asset value (AV): This is the value of an asset that is usually the replacement value. This is not the depreciated value, especially when it is nontangible and cannot be determined by accounting.
2. Exposure factor (EF): This is the financial loss that results from the realization of a threat. It is usually expressed as a percentage value of an asset value. A threat generally does not eliminate the whole asset value, but rather reduces the asset value. Different threats will have different impacts and exposure factors.
3. Single loss expectancy (SLE): The SLE represents the financial loss when a threat scenario occurs once. It is defined as $\mathrm{SLE} = \mathrm{AV} \cdot \mathrm{EF}$.
4. Annualized rate of occurrence (ARO): The ARO is an estimate of how many times an event occurs over one year. If the probability of a threat is once in 10 years, the ARO is 0.1.
5. Annualized loss expectancy (ALE): This is the expected annualized loss of asset value due to the threat. It is defined as $\mathrm{ALE} = \mathrm{SLE} \cdot \mathrm{ARO}$.

Many risk frameworks exist, such as ISO 27005, NIST SP 800-39, and FAIR OCTAVE. They all use quantitative, qualitative, or a combination of both approaches.

Risk management objectives

A variety of risk management objectives are typically used to determine the resources required to continue business operations in case of an event. They mainly represent different time intervals until data or systems and processes are operational. Senior management is involved in creating these objectives, as the time intervals directly translate into operational costs. Therefore, senior management involvement helps to adequately invest in the right resources and prioritize based on business needs. The typical objectives are listed below.

- Recovery time objective (RTO): RTO is the period from the beginning of an outage until the service is operational again. It is a measurable interval of time in which the recovery activities take place. Different business processes will have different RTO targets depending on their priority for the business. A business impact analysis (BIA) can help to establish the RTOs.
- Recovery point objective (RPO): The RPO is the period of acceptable loss of data due to an incident or disaster. This is usually the maximum period between backups or replications in a system. Hours or minutes are normally measured, and as for RTO, shorter periods of time are associated with higher costs.
- Maximum tolerable downtime (MTD): The MTD is a period after which the survival of the organization would be at risk. Organizations often start by defining this measure and then deriving RTO and RPO from it. The MTD should not be interpreted as a target number but rather a point of no return after which the business would have to close.

Other objectives exist based on the needs of the organization.

The Risk Register

Risk registers vary depending on the organization. The table below shows a typical risk register with one sample risk record.

Table 4: Risk Register

Item	Description	Example
ID	unique identifier for the risk record	15081
Status	current status: open, closed, pending, in progress	in progress
Creation date	date that the risk entry was created	2019-10-15
Source	activity or event that was the source of first information: risk assessments, vulnerability management, security incident, threat intelligence, third-parties	vulnerability management
Title	short description of the risk	CRM system OS patch missing
Description	description of the risk	Due to missing patch KB4530691 of the Windows server SRVWNDUS19007, a hacker could get access to the CRM database of the organization.
Threat description	description of the potential threat	An external or internal attacker could exploit the vulnerability, gain root access on the server, and finally impair the confidentiality, integrity, or availability of the CRM database running on that server.
Control	impacted control	patch management
Untreated impact	impact level or value if risk is not treated	high
Untreated probability	probability level or value if risk is not treated	medium
Untreated risk level	risk level if risk is not treated	high risk
Treated impact	impact level or value if risk is treated	high
Treated probability	probability level or value if risk is treated	low
Treated risk level	risk level if risk is treated	medium risk
Risk treatment	chosen method of risk treatment: accept, mitigate, transfer, avoid	mitigate

Item	Description	Example
Risk treatment details	details of the risk treatment	Deploy patch KB4530691 on that Windows server. In the meantime, deploy patch KB4530691 on that Windows server and put the server into a secure zone protected by an IPS system.
Risk treatment planned implementation dates	planned dates when the actions are taken	2019-12-15

Source: Created on behalf of IU (2020).

5.3 The ISO 27K Series

The ISO/IEC 27000-series (also known as the ISMS Family of Standards or ISO27K) consists of information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series provides best practice recommendations on information security management (the management of information risks through information security controls) within the context of an overall information security management system (ISMS). As of January 2020, more than 50 standards within the series have been published and more than 20 are in the making. The scope of the standards is very broad but in parts it is very specific. There are standards that focus on a certain set of technologies or industry sectors.

Organizations can be certified against the ISO 27001 standard, in conjunction with ISO 27002 and ISO 27701. Also, ISO 27017 and ISO 27018 are certifiable. The other ISO 27K standards are not certifiable, but they provide guidance and form a holistic security framework. The table lists the ISO 27K standards that are well known and play a large practical role (SecAware Policies, n.d.).

Table 5: ISO 27k Standards

ISO 27K Standard	Description
ISO/IEC 27000:2018	An overview and introduction to the ISO27K standards, plus a glossary for the specialist vocabulary
ISO/IEC 27001:2013	The Information Security Management System requirements standard, formally specifying a certifiable ISMS
ISO/IEC 27002:2013	The code of practice for information security controls
ISO/IEC 27003:2017	Guidance on how to implement ISO/IEC 27001
ISO/IEC 27004:2016	Information security management measurement
ISO/IEC 27005:2018	Information [security] risk management
ISO/IEC 27018:2019	Concerns Personally Identifiable Information in public clouds

ISO 27K Standard	Description
ISO/IEC 27701:2019	Requirements and Guidance on extending ISO/IEC 27001 and 27002 to manage privacy as well as information security

Source: created on behalf of IU (2020), based on SecAware Policies, n.d.

An ISMS According to ISO 27001

ISO 27001 defines an Information Security Management System (ISMS) (International Organization for Standardization, 2013b). It is the most cited standard in the 27K family and the de facto international standard to prove that cyber security is managed adequately in an organization. The standard consists of ten chapters and an annex. The first three chapters briefly cover the scope, referencing ISO 27000 to define the terminology and the terms used.

In chapter four (context of the organization), the standard requires an organization to understand what the organizational goals are, what the stakeholders of the organization expect, and what their needs are. Also, the scope of the ISMS must be determined. It is crucial to understand that an organization usually narrows the scope of the ISMS to a certain geographical or organizational scope where it applies. The scope can also exclude certain controls in annex A.

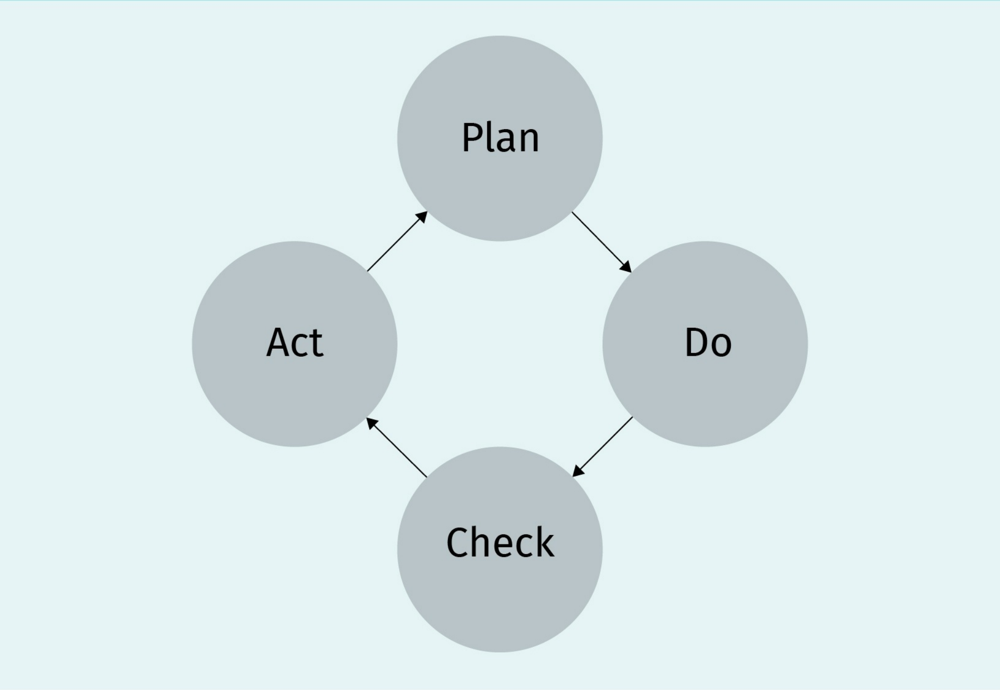
Leadership is covered in chapter five. It requires an organization to demonstrate effective leadership to implement and steer the ISMS. A policy must be drafted that meets the needs of the organization. Also, roles and responsibilities are assigned and communicated.

Planning of the ISMS is covered in chapter six of the standard. The main topic in this chapter is to build and maintain a cyber security risk management system. The mitigations for each risk must be chosen to match the control objectives in annex A. In this chapter, the standard requires an organization to define cyber security objectives and their plans to achieve them.

Having an adequate level of resources is the focus of chapter seven (support). The resources must be able to fulfill their roles and all contributors in the organization need to be aware of the policy and their role in protecting the organization. Information must be documented and undergo document control, which includes regular reviews and version control.

Chapter eight is about operations, risk assessments, and risk treatment. In chapter nine, the ISMS is evaluated. This happens via monitoring, internal audits, and management reviews. Finally, chapter ten introduces continual improvement measures to the ISMS. They should follow the well-known PDCA cycle shown in the figure below.

Figure 12: PDCA Cycle



Source: Created on behalf of IU (2020).

Finally, annex A includes the 144 controls in 14 different groups, starting with **A.5** (International Organization for Standardization, 2013a).

A.5
In ISO 27002, chapter five and following are mapped exactly to the relevant annexes in ISO 27001, so annex A.5 in ISO 27001 maps to chapter five in ISO 27002.

- A.5: Information security policies (two controls)
- A.6: Organization of information security (seven controls)
- A.7: Human resource security (six controls that are applied before, during, or after employment)
- A.8: Asset management (ten controls)
- A.9: Access control (fourteen controls)
- A.10: Cryptography (two controls)
- A.11: Physical and environmental security (fifteen controls)
- A.12: Operations security (fourteen controls)
- A.13: Communications security (seven controls)
- A.14: System acquisition, development, and maintenance (thirteen controls)
- A.15: Supplier relationships (five controls)
- A.16: Information security incident management (seven controls)
- A.17: Information security aspects of business continuity management (four controls)
- A.18: Compliance with internal requirements, such as policies, and with external requirements, such as laws (eight controls)

ISO 27002 includes proposals concerning how to implement these controls. Note that it is not mandatory to use these proposals—others are available such as NIST or the German BSI Baseline Security, IT Grundschutz.

A PIMS according to ISO 27701

ISO 27701 is a relatively new standard that was published in 2019. It is an extension of ISO 27001 and ISO 27002, and describes a privacy information management system (PIMS), sometimes also called data privacy management system (DPMS). An organization can only be certified according to ISO 27701 in conjunction with its ISO 27001 certification. This certification demonstrates that an adequate privacy management system is set up, but it would not satisfy the requirements of a certification against article 42 GDPR.

In chapters one to six, the standard emphasizes how ISO 27001 and ISO 27002 help to protect PII and how to use the same methods, such as policies or risk management, in a PIMS. In chapters seven and eight, additional guidance for both controllers and processors are described. The annex contains 49 additional controls that are relevant to data privacy. The standard also contains a mapping table that shows how the different controls map to legal requirements of GDPR.

The concept is to integrate both ISMS and PIMS into one management system. According to ISO 9001, some organizations also choose to integrate it with quality management.

5.4 IT Security and IT Governance

IT governance and IT security must be aligned with business needs. The importance of this cannot be underestimated as many organizations suffer from silo thinking in that area, leading to unnecessary effort and conflict. An effective security governance program will address several activities and responses.

- Risk management: Ensure that all cyber security risks are adequately addressed and managed.
- Process improvements: Changes are made to business processes that improve security.
- Event identification: Technologies and processes are put in place to identify security events and incidents as quickly as possible.
- Incident response: Incident response procedures that help to avoid incidents and manage them according to risk are put in place, helping to reduce the probability and impact of an incident.
- Improved compliance: All applicable laws, regulations, and standards are re-identified to ensure that the organization maintains compliance.
- Business continuity and disaster recovery planning: Adequate business continuity and disaster recovery plans are maintained and tested regularly.
- Metrics: Key security events such as incidents, changes, policy violations, vulnerabilities, audits, or trainings are measured.
- Resource management: Human and financial resources are allocated to security measures in order to achieve goals.
- Improved IT governance: An effective security governance helps to make better strategic decisions and keeps risk at a tolerable level.

Roles and Responsibilities

Organizations often use **RACI charts** to document the following:

RACI Charts
A RACI chart is not only used in cyber security, but in many other areas of IT and business.

- responsibility (person or role that performs the work).
- accountability (person or role that is ultimately answerable for the activity, often a manager).
- consulted (roles that need to be consulted, such as experts).
- informed (roles that need to be informed about a certain activity or decision).

A typical RACI chart for a cyber security user account request can look like this:

Table 6: RACI Chart

Activity	User	Service desk	Manager	Security team
Request user account	R	I	A	I
Approve user account	I	C	A	C
Provision user account	I	R	I	I

Source: Created on behalf of IU (2020).

When designing RACI matrices, a segregation of duties needs to be considered so at least two roles or people have to execute a critical task. Also, conflicts of interest need to be avoided, e.g., an approver cannot be the same person that executes the task or requests it.

Roles in, or related to, a security organization typically include

1. chief information security officer (CISO). This is the highest ranked role in the security organization and is typically part of the board, or at least reports directly to them. To avoid conflicts of interest, the CISO should not report to the CIO.
2. chief privacy officer (CPO). Organizations that manage a huge amount of PII often appoint a CPO who safeguards the PII of the organization. Sometimes, a CPO can also be the assigned DPO where legally required.
3. security audit manager. This role is responsible for the audits in the security area—they schedule and manage audits.

There are many other roles that collaborate with cyber security in IT, risk management, and other areas of the business.

Control Frameworks

Governance frameworks do not need to be invented for each organization and many are available that help to manage the IT objectives of an organization. Some widespread examples of such frameworks are listed below.

- COBIT: This stands for Control Objectives for Information and Related Technology. It is an IT management and governance framework developed by ISACA, primarily focusing on IT governance (although security processes are also part of its framework). The four COBIT domains are
  a) align, plan, and organize (APO);
  b) build, acquire, and implement (BAI);
  c) deliver, service, and support (DSS); and
  d) monitor, evaluate, and assess (MEA) (ISACA, 2019).
- ISO/IEC 27K: This is family of standards for cyber security management.
- ISO/IEC 38500: This is an international standard on the governance of IT.
- ITIL & ISO/IEC 20000: The IT infrastructure library (ITIL) is a framework including IT operational processes, such as security, in its framework. ISO/IEC 20000 is a certifiable standard that is adopted from ITIL. The framework focuses on managing IT services.
- HIPAA: The United States Health Insurance Portability and Accountability Act requires the protection of health information and the management of technical, administrative, and physical safeguards.
- NIST SP 800—53: The United States National Institute for Standards and Technology (NIST) special publication 800—53 is one of the most well-known security frameworks, and is mandatory for all United States public sector information systems. Many other organizations have also adopted those controls outside the public sector.

5.5 Example: IT Security for Credit Cards (PCI DSS)

An example of a security framework is PCI DSS, the payment card industry data security standard. Credit card companies such as VISA and American Express founded the standard to ensure that credit card transactions are adequately secured and risk is reduced in the card payment process.

The following are in scope:

- Systems that store, process, or transmit card holder data
- Systems that provide security functionalities or may impact the security of card holder data
- Any other component or device located within, or connected to, card holder data environment (CDE)

The standard applies to cases where the primary account number (PAN) is stored or processed. The standard does not permit the storage of sensitive authentication data, including the data of the magnetic strip of a card, the card control numbers, or the PIN. The standard mainly consists of twelve high level requirements where PCI DSS sets controls detailing rules that an organization that processes cardholder data must obey. The high-level requirements are as follows:

- install and maintain a firewall configuration to protect cardholder data,

- do not use vendor-supplied defaults for system passwords and other security parameters,
- protect stored cardholder data,
- encrypt transmission of cardholder data across open public networks,
- protect all systems against malware and regularly update anti-virus software or programs,
- develop and maintain secure systems and applications,
- restrict access to cardholder data by business need to know,
- identify and authenticate access to system components,
- restrict physical access to cardholder data,
- track and monitor all access to network resources and cardholder data,
- regularly test security systems and processes, and
- maintain a policy that addresses information security for all personnel.

For each of the requirements, specific test procedures are set out that help to prove that an organization is compliant with the standard. They are audited before an organization is allowed to process credit card data, and these audits are rigorous.

SUMMARY

Cyber security must be managed. An adequately structured security policy addresses the whole organization and ensures that everyone understands their duties. It makes security enforceable and needs to be policed, i.e., audited. Noncompliance has consequences and must be documented.

Risk management plays an integral role in all cyber security frameworks and in managing security. It can have several forms. A holistic risk management process ensures that risks are identified and adequately prioritized. The four risk treatment strategies help to find an adequate treatment. Keep in mind that risk is part of business, and every business has a certain risk tolerance.

The ISO 27K family of standards are general, specific, and constantly in development. ISO 27001 is especially helpful when building an information security management system (ISMS). IT governance and security governance work together to foster good decisions within the business. Frameworks such as COBIT or NIST SP 800—53 can help an organization to find appropriate structures and controls. Finally, PCI DSS is a mandatory standard for organizations that processes credit card data. It has a rigid set of requirements and controls that help to secure credit card details and therefore reduce the risk in the payment card industry for both the industry and cardholders.

UNIT 6

CRYPTOGRAPHY

STUDY GOALS

On completion of this unit, you will have learned …

- the basic concept of cryptography.
- the main concepts of symmetric and asymmetric encryption.
- how and why to use one-way functions and hashing algorithms.
- the main problems with the key exchange process.
- why cryptography is so important for ICT processes.

6. CRYPTOGRAPHY

Introduction

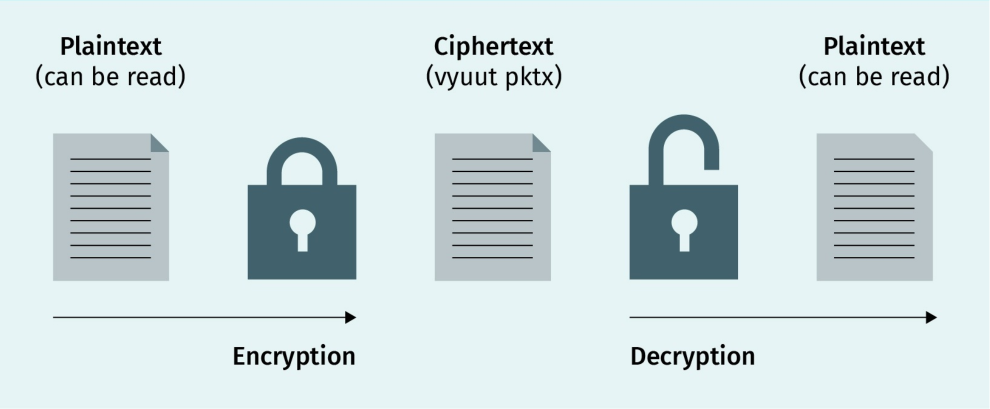
One of the first known uses of cryptography was in Roman times. When Caesar sent messages to his army, he replaced every “A” in his messages with “D,” every “B” with “E,” etc., because he did not trust the messengers. Only those who knew the encryption system could read the message (i.e., “shift by 3” system). For example, “we will attack tomorrow morning” would result in a message reading “zh zloo dwwdfn wrpruurz pruqlqj” after being encrypted using Caesar’s method.

Cryptography is essential in the security domain and, in this unit, we will try to explain some of the most important concepts.

Some terms must be clarified before we jump into the world of cryptography.

- “Plaintext” is information or a text that can be directly read by humans or a machine.
- “Ciphertext” is the result of an encryption process—this text cannot be read without a special algorithm (cipher). Without the cipher, the ciphertext looks like a meaningless message. A cipher is a mathematical function used in the encryption/decryption process.
- A “key” is a phrase, number, word, or combination that is used to encrypt plaintext or decrypt a ciphertext.
- “Encryption” is the process of translating plaintext into ciphertext.
- “Decryption” is the opposite process—this is the process of converting ciphertext into its original form.
  The figure below shows the process of encryption and decryption, as well as the role of plaintext and ciphertext.

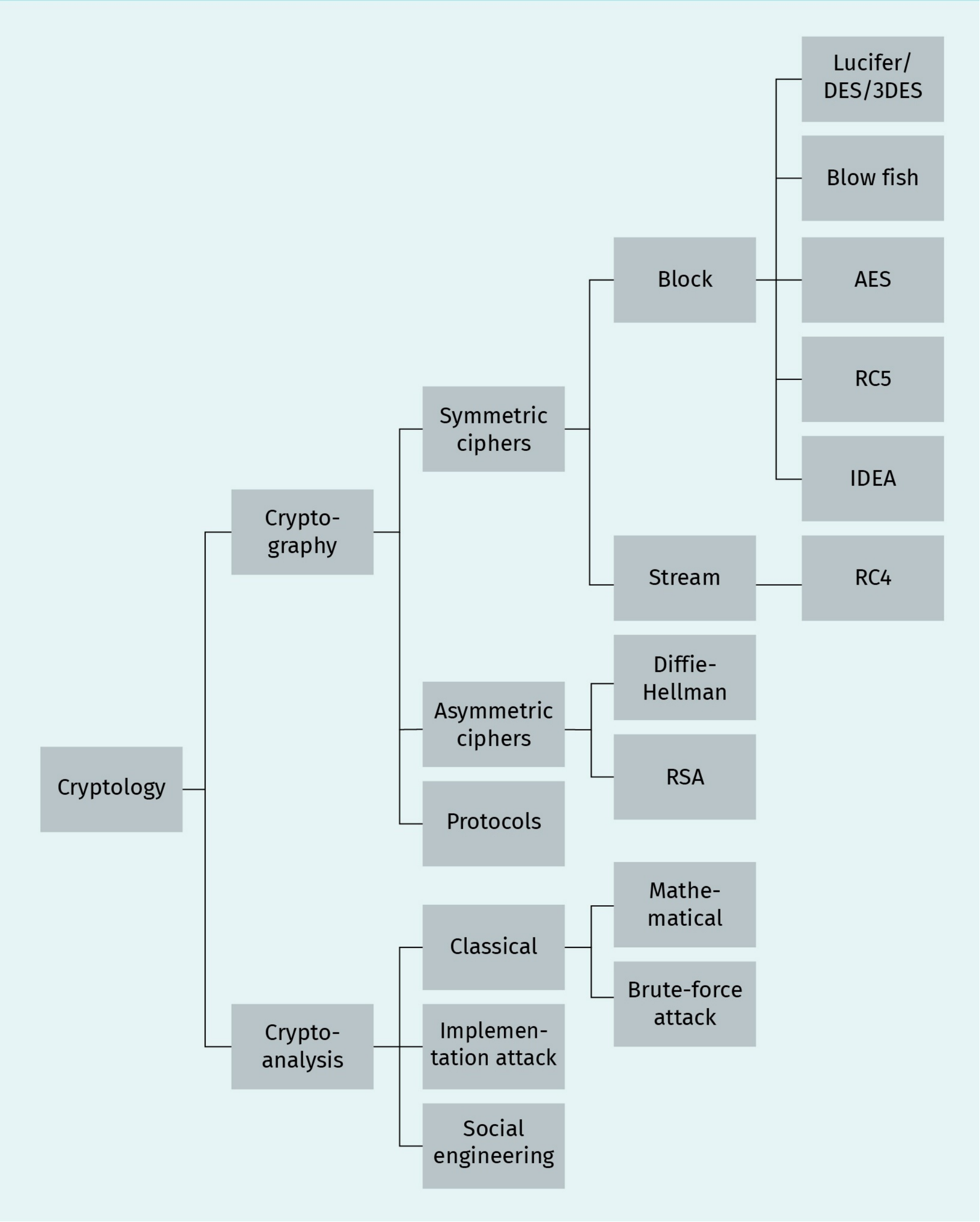
Figure 13: Encryption and Decryption Process



Source: Created on behalf of IU (2020).

- “Cryptography” is the science of using mathematical methods to securely encrypt data. Cryptography is important in information and communications technology (ICT) and the cyber security domain because it helps us to store sensitive data and transmit it through an insecure network (LAN, WAN, Intranet, Internet, etc.).
- “Cryptoanalysis” is the science of analyzing and breaking this encrypted communication.
- “Cryptology” is the science of creating and breaking ciphers.
- “Cryptosystem” is a system that consists of a cryptographic algorithm, all keys, combinations, and protocols. One example of a cryptosystem is Pretty Good Privacy (PGP).

Figure 14: Cryptology Overview



Source: Created on behalf of IU (2020).

Classification of cryptographic algorithms can be done in several ways; in this unit, we will use the simple classification method—“number of keys.”

6.1 Symmetric Cryptography

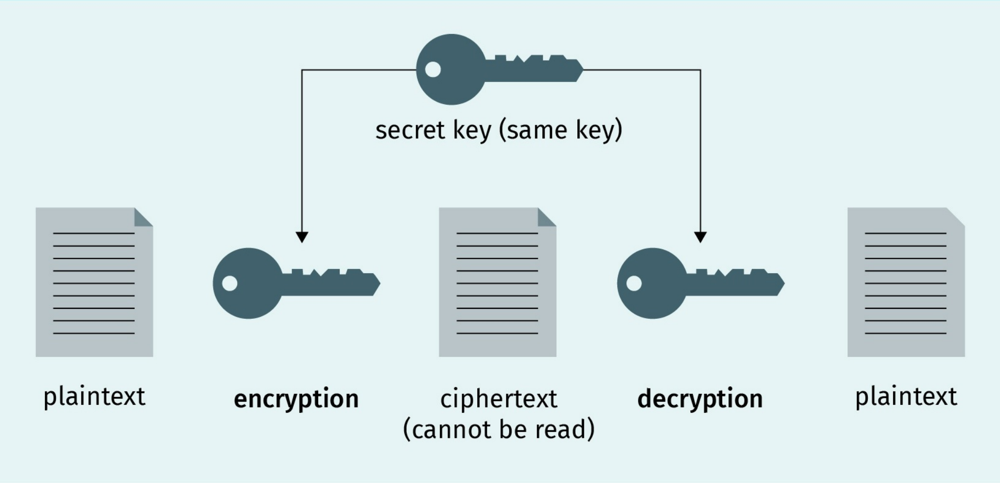
The first type of algorithm we will talk about is symmetric cryptography or secret key cryptography (SKC). This is an example of symmetric encryption because a single key is used for both encryption and decryption.

In symmetric encryption, the sender uses the “secret” key to encrypt the plaintext and then sends the ciphertext to the receiver. The receiver must apply the same secret key to decrypt the message and recover the original plaintext, as shown in the figure below. With this form of cryptography, the key must be known to both the sender and the receiver. The biggest difficulty when taking this approach is the distribution and management of the keys (Kessler, 2020). Using a secret key cipher means that you must exchange a separate key with each communication partner, even for a short message, resulting in a large number of keys that must be managed by each user.

A one-time pad is the only proven non-decryptable encryption technique available. The key length must be at least the same size as the plaintext. The key must be random and must only be used once. One-time pads were used before the invention of computers and they are still used today when encryption and decryption are done by hand. One-time pads might play a role in quantum cryptography that goes beyond the scope of this unit.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers.

Figure 15: Symmetric Encryption



Source: Created on behalf of IU (2020).

Stream cipher schemes operate on a single bit (or byte) at a time, encrypting each bit individually. Most stream ciphers implement some form of feedback mechanism so that the key is constantly changing. Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous *n* bits in the keystream. It is called “self-synchronizing” because the decryption process can remain synchronized with the encryption process merely by knowing how far into the n-bit keystream it is (Kessler, 2020). Synchronous stream ciphers generate the keystream so that it is independent of the message stream, but the sender and the receiver use the same keystream generation function. While stream ciphers do not propagate transmission errors, they are naturally periodic, meaning that the keystream will eventually repeat.

A block cipher scheme encrypts one fixed-size block of data at a time. A block is a fixed number of bits. Most block ciphers convert a block of plaintext into a ciphertext block of the same size by applying a key and a method that is invertible. There are different ways how to combine the individual blocks in a sequence of blocks, defined by different block cipher modes.

In a block cipher, a plaintext is split into a sequence of blocks of the same length (typically 32, 64 or 128 bits) which are then encrypted separately. There are different ways how to encrypt the individual blocks in a sequence of blocks, defined by different “block cipher modes”. Apart from the electronic codebook mode ECB described below, all other modes use additional information such as the previous block or a counter in order to ensure that the same plaintext does not lead to the same ciphertext when encrypted using the same key. The resulting block cipher modes differ considerably in their properties, including their security, the effects of individual bit errors or lost blocks on other blocks, and whether encryption and / or decryption can be sped up by working on different blocks in parallel.

There are several common block cipher modes (Paar & Pelzl 2010, p. 124-134):

- ECB: Electronic codebook is the simplest and most obvious block cipher mode. Each block is encrypted separately using the secret key, and the same plaintext block will always lead to the same ciphertext block. This ensures that bit errors in transmission only affect a single block, and allows different blocks to be encrypted and decrypted in parallel. However, it is quite insecure since the same plaintext block always leads to the same ciphertext block, which allows a number of attacks such as brute-force attacks or the unnoticed substitution or insertion of blocks. Even without being able to decrypt a block, it may provide important information to an attacker to know that the same message block was sent repeatedly.
- CBC: Cipher block chaining is a commonly used mode of operation where every block of plaintext is “XOR-ed” with the previous ciphertext block (or a random block called initialization vector in the case of the first block) before being encrypted. This implies that every ciphertext block depends on all plaintext blocks processed before this operation as well as on the initialization vector.

The following three block cipher modes all work by adding a sequence of key-dependent blocks to the plaintext rather than encrypting the plaintext itself. This has the advantage that they can also be used as a stream cipher, because the resulting cipher text can be created bitwise rather than blockwise.

- OFB: Output feedback uses an initialization vector plus the key to generate a sequence of blocks that are then added bitwise (XOR-ed) to the plaintext.

- CFB: Cipher feedback works similarly but additionally uses the ciphertext of the previous block to generate the sequence of blocks added to the plaintext.
- CTR: Counter mode uses a counter and an initialization vector to generate the sequence of blocks added to the plaintext.

Table 7: Most Common Symmetric Encryption Algorithms

Algorithm	Key length (bits)	Block size (bits)
DES	56	64
3DES	56,112,168	64
AES	128,192,256	128
IDEA	128	64
RC4	40—256	Stream cipher
RC5	0—2040	32,64,128
Blowfish	32—448	64
Twofish	To 256	128
Safer+/++	128	64/128

Source: Created on behalf of IU (2020).

The table above shows ~~us~~ some of the most used symmetric encryption algorithms alongside their key length and block size (in bits).

DES was the dominant symmetric encryption algorithm from the mid-1970s to the mid-1990s. DES is a good example of a block cipher that is very efficient in hardware implementation.

However, today, a standard DES with a 56-bit key length can be broken relatively easily and, because of that, triple DES (3DES) was created, which involves encryption with DES three times in a row (Paar & Pelzl, 2010). Until a few years ago, it was considered to be certain that there was no possible practical attack against 3DES.

The 3DES algorithm applies its keys as follows:

- encrypting with the first key (k1),
- decrypting with the second key (k2), and
- encrypting with the third key (k3).

There is also a two-key variant, where keys k1 and k3 are the same.

In 2016, researchers found a new way to recover and decrypt cookies from HTTPS authentication sessions encrypted with 3DES. The weakness of Sweet32 was made public, and this research exploited a known vulnerability to collision attacks in 3DES, which may become possible during lengthy transmissions, the exchange of content files, or transmissions vulnerable to text injection (Karthikeyan & Gaëtan, 2016). After the exposure of this vulnerability, NIST proposed in the standard 800-131A that 3DES be deprecated. The document "Transitioning the Use of Cryptographic Algorithms and Key Lengths" (Barker & Roginsky, 2019) formalizes the retirement of triple DES by the end of 2023. After this, 3DES will only be recommended for legacy use, which means decryption only.

Today, the most used symmetric algorithm, which is now the default, is the Advanced Encryption Standard (AES) and its variants AES-128, AES-192, and AES-256. AES was introduced in 2001 to replace 3DES. AES allows us to choose a 128-bit, 192-bit, or 256-bit key (for very high security requirements), where the security of a key grows exponentially with its size. AES is used in many applications, and it is the algorithm trusted as the standard by the United States government as well as numerous other organizations. AES is efficient in software and hardware. Today, we can see AES implementation in messaging apps such as WhatsApp and Signal, applications like VeraCrypt and WinZip, and also in a range of hardware. AES was originally known as the "Rijndael" block cipher, developed by Joan Daemen and Vincent Rijmen, two cryptographers from Belgium, until it was chosen by NIST as the new standard successor to DES and then renamed AES. Reasons for selecting Rijndael were its widespread abilities, including its performance on both hardware and software, ease of implementation, and its level of security. AES was named the United States federal standard in 2002 and became the standard encryption algorithm for the whole world.

The figure below depicts a memory stick with integrated AES256 encryption integrated in chip.

Figure 16: USB Memory Stick with AES256 Encryption in Chip

Source: Vatiga.com, 2020.

6.2 Asymmetric Cryptography

Symmetric cryptography is a very old practice and has been used since Roman times when there was only one key for encryption and decryption. However, asymmetric encryption, or public key cryptography, is relatively new—the general concept was first presented in 1976. In this kind of encryption, there are two keys (one pair)—a public key that may be disseminated widely and a private key which is only known to the owner. In the PKC system, anyone can encrypt a message using the receiver's public key. Encrypted messages can only be decrypted with the receiver's private key—this may be compared to a mailbox on the street. The mailbox is public meaning that anyone who knows its location (public key) can go to it and put in a letter, but only the owner of the mailbox has a physical key (private key) which allows them to access the mailbox and read the letters.

Asymmetric cryptography uses trapdoor functions. A trapdoor function is easy to compute in one direction but difficult in the opposite or inverse direction. The best-known algorithm for PKC is the Rivest, Shamir, and Adleman (RSA) algorithm. The RSA algorithm generates a pair of "public and private keys." Those keys are mathematically linked to each other. Public keys are used to encrypt data, and only the corresponding private key can be used to decrypt it. Knowing the public key does not enable a crypto analyst to reveal the private key. The algorithm is based on Euler's totient function. $\varphi(n)$ is the number of integers k in the range $1 \leq k \leq n$ for which the greatest common divisor $\gcd(n, k)$ is equal to 1.

The **algorithm** consists of the following steps:

Algorithm
The open source tool CrypTool can be used to experiment and visualize cryptographic algorithms.

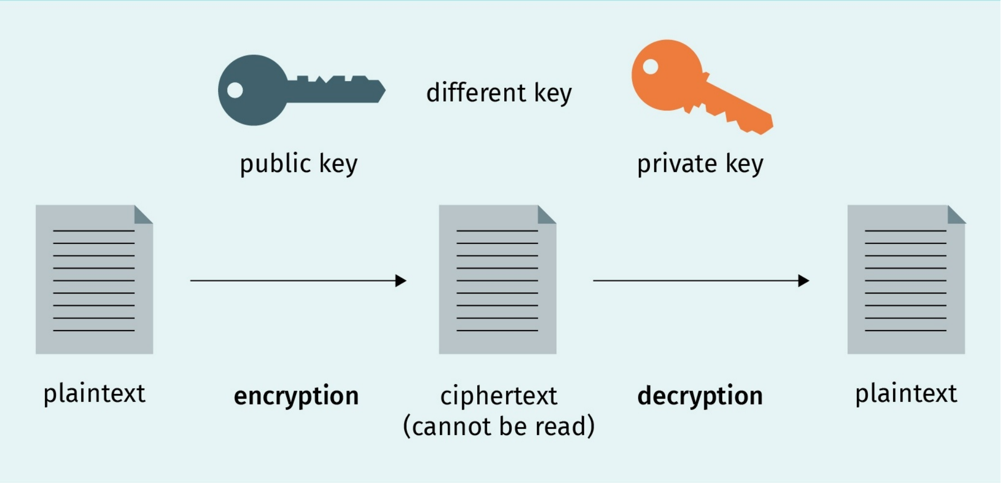
- Choose two big prime numbers p and q.
- Calculate $n = pq$.
- Choose a small, odd, natural number e, that is relative prime with $\varphi(n) = (p-1)(q-1)$. Put differently, the greatest common divisor is $(e, \varphi(n)) = 1$.
- Calculate d as the solution to the equation $ed \bmod \varphi(n) = 1$. The Euclidian algorithm can be used for this.
- The pair $P = (e,n)$ is the public key.
- The pair $S(d,n)$ is the private key.

The RSA algorithm is applied by

- encryption of the message M:$E(M) = M^e \mathrm{mod}\ n$, and
- decryption of the ciphertext C:$D\left(C\right) = C^d \mathrm{mod}\ n$.

It can now be shown mathematically that $D(E(M)) = M \bmod n$ and $E(D(C)) = C \bmod n$.

Figure 17: Asymmetric Cryptography (Public Key Cryptography)



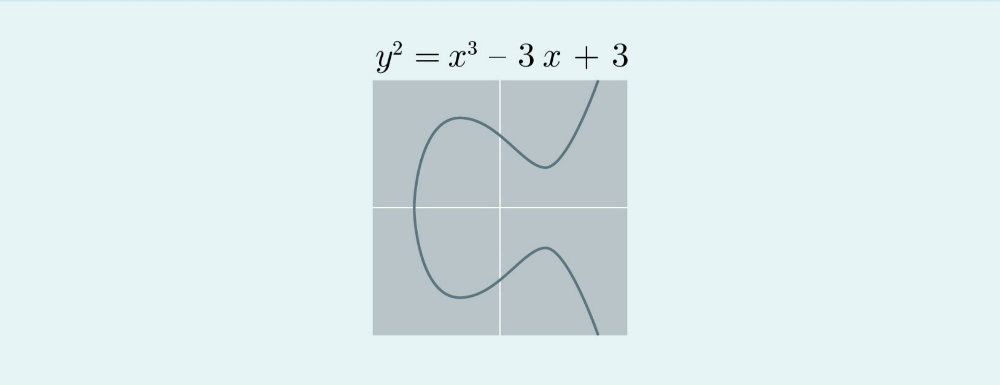
Source: Created on behalf of IU (2020).

As we can see in the figure above, the sender and receiver want to exchange a message (plaintext) via an unsecured communication channel, for example, the internet. The sender uses a receiver's public key to encrypt a message and sends a cipher to the receiver who then uses their own private key to decrypt a message. In order to encrypt a text with the receiver's public key, a receiver must make this key available to the sender, but receivers never distribute their own private key.

To deliver confidentiality, integrity, authenticity, and non-reputability, users and systems need to be sure that a public key is authentic. This means that one needs to be sure that the public key belongs to the correct person or entity and that it has not been tampered with or replaced by a malicious third party. In a Public Key Infrastructure (PKI), trusted Certificate Authorities (CA) certify ownership of key pairs and certificates in order to authenticate the digital identities of the users. Encryption products based on the Pretty Good Privacy (PGP) model (i.e. OpenPGP) rely on a decentralized authentication model called a "web of trust." The web of trust is a concept that provides authenticity by binding a public key to its owner. It does not rely on a central authority, but rather on trust between the users of the network.

6.3 Elliptic-Curve Cryptography

Figure 18: Example of an Elliptic Curve



Source: Created on behalf of IU (2020).

The challenge with RSA is that factoring algorithms becomes more efficient as the size of the numbers being factored gets larger. Hence, the key lengths that must be used for RSA get larger and larger, so specifically for small devices or smart cards, this is not a long-term sustainable solution.

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography to provide an equivalent level of security.

The math is not as simple as factoring and will not be covered in this course. In this field of mathematics, points on the curve compose a structure called a group. It uses the horizontal symmetry of every elliptic curve and the fact that when a line is drawn that connects two points on the curve, it will intersect with the line at exactly one more place. Now we use the symmetric structure of the curve to derive the dot at the other side of the symmetry axis of the curve. It turns out that if you have two points, an initial point “dotted” with itself n times to arrive at a final point, finding out *n* when you only know the final point and the first point is hard. If we only have the resulting point of that operation, it is extremely difficult to understand what combination of other dots provided this result; hence, we have a trapdoor function.

6.4 Hash Function

In mathematics, a hash function maps data of a variable input size onto an image of fixed size. It is therefore usually not reversible. The image is called hash or digest. A pure mathematical hash function is not resistant to cryptographic attacks as it is not designed for cryptography.

Hash Function
A hash function is a "one-way" function that generates the "hash" of a file.

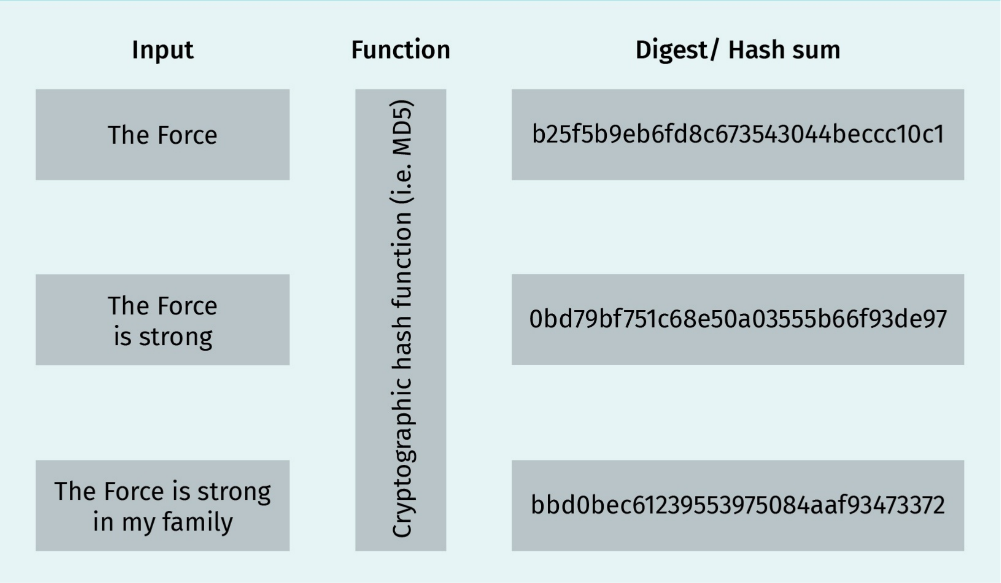
A cryptographic **hash function** is resistant to a number of cryptographic attacks. They employ

- pre-image resistance. For a given h in the output space of the hash function, it is hard to find any message x with $\mathrm{H}(\mathrm{x}) = \mathrm{h}$. This is an alternative way of stating that H must be a one-way function.
- second pre-image resistance. For a given message x_1 it is hard to find a second message $\mathrm{x}_2 \neq \mathrm{x}_1$ with $\mathrm{H}(\mathrm{x}_1) = \mathrm{H}(\mathrm{x}_2)$. This is also called weak collision resistance.
- collision resistance. It is hard to find a pair of messages $\mathrm{x}_1 \neq \mathrm{x}_2$ with $\mathrm{H}(\mathrm{x}_1) = \mathrm{H}(\mathrm{x}_2)$.

It is clear that if pre-image resistance is not achieved, collision resistance cannot be achieved.

Cryptographic hash functions, or message digests (MD), are algorithms that use no keys. Ideally, it is practically impossible to recover the original content of a hashed file. This is the most important difference between "hashing" and "encryption." Hash algorithms are typically used to provide a "digital fingerprint" of a file, which is often used to ensure file integrity and make sure that the file has not been altered by a virus or an intruder. Hash functions are also used by many operating systems to store passwords securely.

Figure 19: Hash Function


Input
Function
Digest/ Hash sum
The Force
The Force is strong
The Force is strong in my family
Cryptographic hash function (i.e. MD5)
b25f5b9eb6fd8c673543044beccc10c1
0bd79bf751c68e50a03555b66f93de97
bbd0bec61239553975084aaf93473372

Source: Created on behalf of IU (2020).

We can try to experiment with a string: "IUBH." As a result of hashing with the MD5 function, we will get the "34d4d02d2f87b03e94ec3754b64f1392" string. The string "IUBH is your future" results in the MD5 digest "badae2ff12f456a2da21328d982670a6". The hash is the same size but is completely different from the previous hash. Commonly used words and their hashes are included in rainbow tables, which are used to hack password files and derive the original passwords.

There are many different hash functions, but the most popular ones are the MD4 family. MD5, SHA, and RIPEMD are based on the MD4 algorithm. MD4 was an innovative idea proposed by Ronald Rivest, and MD5 is a strengthened version that was also proposed by Rivest in 1991. MD5 became widely used, for example, in internet security protocols, for computing checksums of files, or for storing of password hashes. In 1993, NIST published a new MD standard called Secure Hash Algorithm (SHA). The first version was SHA-0, later renamed SHA-1, which is a replacement for MD5 as it turned out to no longer be secure. In 2001, NIST introduced three more variants of SHA-1: SHA-256, SHA-384 and SHA-512, with message digest lengths of 256, 384, and 512 bits, respectively. In 2004, SHA-224 was introduced to fit the security level of 3DES. These four hash functions are often referred to as SHA-2.

Table 8: MD4 Family of Hash Functions

Algorithm		Output [bit]	Input [bit]	No. of rounds	Collisions found
MD5		128	512	64	yes
SHA-1		160	512	80	not yet
SHA-2	SHA-224	224	512	64	no
	SHA-256	256	512	64	no
	SHA-384	284	1024	80	no
	SHA-512	512	1024	80	no

Source: Paar & Pelzl, 2010.

Similar to the selection of Rijndael as the standard symmetric encryption algorithm (which was then named AES), the United States standards organization set up a competition for a new cryptographic hash algorithm which led to the KECCAK algorithm being selected in 2012 as the new SHA-3 algorithm. Four fixed-length hash algorithms were defined: SHA3-224, SHA3-256, SHA3-384, and SHA3-512, as well as two closely related “extendable-output” functions (XOFs) SHAKE128 and SHAKE256.

Currently, only the four fixed-length SHA-3 algorithms are approved hash algorithms, providing alternatives to the SHA-2 family of hash functions. The XOFs can be specialized to become hash functions, subject to additional security considerations. Guidelines for using the XOFs will be provided in the future (National Institute of Standards and Technology, 2019).

Table 9: SHA-3 Family

Name	Hash length (output)	Block size	Capacity	Security strengths (bits)
SHA3-224	224	1152	448	224

Name	Hash length (output)	Block size	Capacity	Security strengths (bits)
SHA3-256	256	1088	512	256
SHA3-384	384	832	768	384
SHA3-512	512	576	1024	512
SHAKE128	variable (n)	1344	256	min (n, 128)
SHAKE256	variable (n)	1088	512	min (n, 256)

Source: Created on behalf of IU (2020).

Some of the previously used hash functions are not resistant to collision. An example is SHA-1, where it was shown that several documents that produced the same hash value could be created. It should not be used any longer. At the time of writing, SHA3 is the most reliable option.

6.5 Secure Key Exchange

As previously mentioned, one of the main problems in secure communication is how to exchange a key between two parties that need to exchange encrypted information (i.e. sender and receiver). This method of exchanging a key is also known as secure key exchange or key establishment.

In symmetric cryptography, there is only one key, the secret key, that needs to be exchanged. This means that the sender and receiver, in order to communicate confidentially, must exchange the secret key before exchanging encrypted messages. In asymmetric cryptography, on the other hand, the private and secret key are used, and we need to know the other person's public key. The private key should stay private and is not exchanged. In situations where there is more than one person with whom we communicate, a system for key management—the Cryptographic Key Management System (CKMS) —must be established. CKMS must specify rules for this information that will protect the confidentiality, integrity, availability, and authentication of sources. CKMS consists of key exchange, storage, and use. Key exchange is a process in which cryptographic keys are exchanged between the sender and receiver using a cryptographic algorithm.

The Diffie-Hellman key exchange protocol was published in 1976 by Whitfield Diffie and Martin Hellman (based on Ralph Merkle's concepts). According to the contribution of student Ralph Merkle in 2002, Hellman suggested the algorithm be called "Diffie–Hellman–Merkle" key exchange. The Diffie-Hellman key exchange allows users (parties who have not previously met) to securely exchange keys, even if they are using an insecure connection (Diffie & Hellman, 1976). Like other asymmetric cryptosystems, the secrecy of this key exchange is guaranteed due to the use of a one-way function, in this case the discrete logarithm. This was the first asymmetric cryptosystem published, and until then, only symmetric cryptosystems were known.

The Diffie-Hellman key exchange is one of the most commonly used methods to safely distribute keys, and because of that, it is frequently implemented in security protocols such as TLS, IPsec, SSH, or PGP. This makes it an integral part of our secure communications. In practice, the Diffie-Hellman key exchange is rarely used by itself because it does not provide any authentication—without authentication, users are vulnerable to Man-in-the-Middle (MitM) attacks. Because of this, Diffie-Hellman is often implemented in combination with RSA or other algorithms to provide authentication for the connection (Lake, 2019).

The Diffie-Hellman algorithm works as follows.

1. Alice and Bob, who want to exchange a key, agree on a huge prime number n and a huge figure g. Those numbers can be public.
2. Alice chooses a random number x and sends $\mathrm{X} = \mathrm{g}^{\mathrm{x}} \bmod \mathrm{n}$ to Bob. $(\mathrm{X},\mathrm{g},\mathrm{n})$ is her public key and $(\mathrm{x},\mathrm{g},\mathrm{n})$ is her private key.
3. Bob chooses a huge random number y and sends $\mathrm{Y} = \mathrm{g}^{\mathrm{y}} \bmod \mathrm{n}$ to Alice. $(\mathrm{Y},\mathrm{g},\mathrm{n})$ is his public key and $(\mathrm{y},\mathrm{g},\mathrm{n})$ is his private key.
4. Alice calculates the secret key $\mathrm{k} = \mathrm{Y}^{\mathrm{x}} \bmod \mathrm{n}.$
5. Bob calculates the secret key $\mathrm{k'} = \mathrm{X}^{\mathrm{y}} \bmod \mathrm{n}.$

Hence $\mathrm{k} = \mathrm{k'}, \text{as } \mathrm{k} = \mathrm{Y}^{\mathrm{x}} \bmod \mathrm{n} = \mathrm{g}^{\mathrm{xy}} \bmod \mathrm{n} = \mathrm{X}^{\mathrm{y}} \bmod \mathrm{n} = \mathrm{k'}.$

A crypto analyst eavesdropping the connection knows $\mathrm{n},\mathrm{g},\mathrm{X},\mathrm{Y}$ but not k. The crypto analyst tries to solve the equations $\mathrm{Y} = \mathrm{g}^{\mathrm{y}} \bmod \mathrm{n}$ and $\mathrm{X} = \mathrm{g}^{\mathrm{x}} \bmod \mathrm{n}$ to get x and y. This is possible but very difficult and is known as the problem of discrete logarithms.

Perfect forward secrecy (PFS) is a “key-agreement” protocol that uses a unique public key for each session between a client and a server, or between two users, for example. The key that results is never used to derive another key. This ensures that a current session cannot be compromised by using a key derived from any previous session, and previous sessions cannot be decrypted by anyone who manages to acquire the current key (Villanova-University, 2019). This key-agreement protocol uses complex mathematical processes and discourages brute force hacking attempts. Even if an attacker somehow came into possession of a session key, the worst that could happen is that the attacker gains access to a single session.

Steganography

Steganography is a method of secretly hiding a message within another medium. The main goal is to avoid the detection of the message, but that message could be encrypted using the same methods mentioned previously. One of the easier methods is the least significant bit (LSB) method. With this method, usually used on an image or video stream, the last bit of the color coding is changed. The change is not visible to the human eye; hence, it hides the message. However, this method is also easy to detect if an analyst is looking for it, and more sophisticated methods are available.

SUMMARY

In this unit, the concept of symmetric and asymmetric cryptology is introduced, along with an explanation of how they work. It introduces the concept of a trapdoor function as the basis for asymmetric cryptography, implemented by factoring and by elliptic-curve cryptography. Hash functions are also discussed, while additionally covering de-hashing. Finally, secure key exchange and methods of executing it are described.

UNIT 7

CRYPTOGRAPHIC APPLICATION

STUDY GOALS

On completion of this unit, you will have learned …

- basic concepts of applied cryptography and cryptographic application.
- about Secure Internet Protocol(s).
- how cryptography can be applied in internet security.
- why applied cryptography is so important for IT processes.

7. CRYPTOGRAPHIC APPLICATION

Introduction

Cryptography was, for a long time in history, an esoteric science with very few practical applications. It was used by the military and governments, but without proper computing power, it never reached the masses. In the first part of the 20th century, electromechanical encryption machines were invented, the most famous being the ENIGMA, which was used in World War II by the Axis forces. With the internet revolution starting in the 70s, it became apparent that cryptography is necessary to secure the privacy of users and to enable modern business models such as e-commerce. Nowadays, cryptography plays a crucial role in our day to day lives. For example, over 80 percent of internet traffic is encrypted, encryption is used in electronic payments, and private communication via email or chat services relies on encryption for safety. Law enforcement bodies are challenging the use of encryption and trying to find ways to collect evidence, hence attempting to decrypt data. Finally, cryptography enabled the blockchain technology, which might change the way that transactions occur in the future.

7.1 Digital Signatures

When exchanging documents, a signature provides evidence that the integrity and authenticity of that document is valid. Seals, stamps, and putting initials on each page further strengthen this. A digital signature transports those methods into the electronic world using cryptography.

Digital signature
With digital signature, we can verify authenticity and integrity and achieve non-repudiation.

A **digital signature** is a cryptographic operation where a sender seals a message or file using their identity. Digital signatures are used to authenticate a message and ensure its integrity; however, they do not protect the confidentiality of a message or replace encryption. Digital signatures work by encrypting the hashes of messages. Recipients verify the integrity and authenticity by decrypting the hashes and comparing with the original message.

A digital signature also provides non-repudiation, meaning that the sender cannot dispute its authorship or validity of the document. A digital signature serves the same purpose as a handwritten signature, but it must be emphasised that a handwritten signature is much easier to counterfeit. Another reason that the digital signature is superior and nearly impossible to counterfeit is that a digital signature attests the integrity of the message as well as the identity of the signer (PGP, 2002).

According to NIST, an electronic signature is a cryptographic mechanism used to verify the origin (authenticity) and contents (integrity) of a message (Gutmann & Roback, 1995). The difference between a digital signature and an electronic signature is in the method of identifying businesses and signers. Digital signatures embed Public Key Infrastructure (PKI) into the signing process to identify both the party requesting a signature and the party that provides one. Both the electronic signature and the digital signature are equally capable of identifying a signer, and they are both legally considered signatures, depending on the legislation they are used in. An example is the electronic identification, authentication, and trust services (eIDAS) directive in the European Union, “regulation (EU) No 910/2014 of the European parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC” (European Union, 2014, p. 73). Other legislations have implemented similar regulations.

A digital signature is one of the most important cryptographic tools that is widely used today. Applications that currently use a digital signature include e-commerce, the legal signing of contracts, and secure software updates (Paar & Pelzl, 2010).

The following list details the security goals that are achieved with electronic signatures.

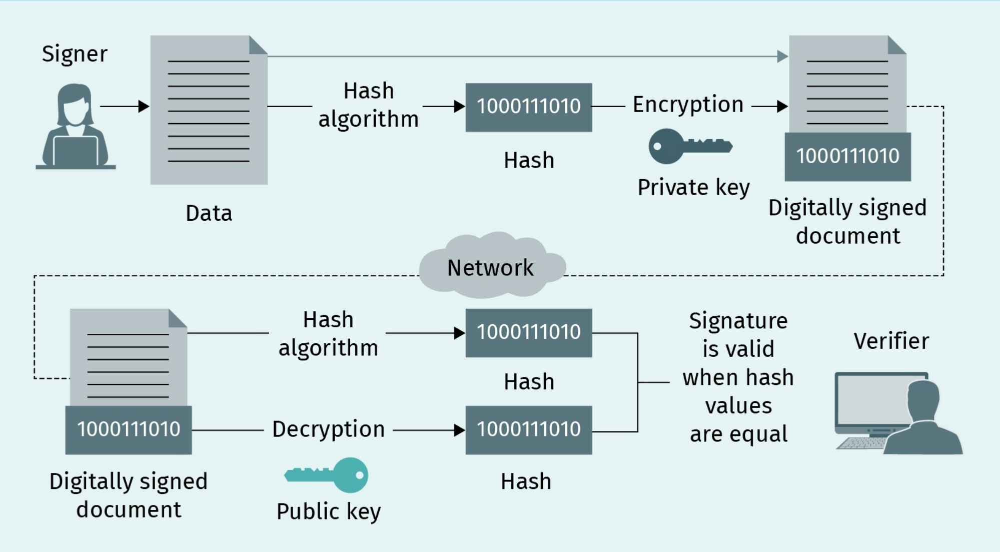
- Integrity: Messages have not been modified in transit.
- Message authentication: The sender of a message is authentic. An alternative term is data origin authentication.
- Non-repudiation: The sender of a message cannot deny the creation of the message (Paar & Pelzl, 2010).

In addition to the four core security services, the following list includes some other security services that are often implemented in combination with electronic signatures.

- Confidentiality is not directly supported by digital signatures but is typically part of a public key infrastructure solution, so it is implemented with the same pair of keys.
- Identification/entity authentication: Establishes and verifies the identity of an entity, for example, a person, a computer, or a credit card.
- Access control: Restricts access to the resources for privileged entities.
- Availability: Provides assurance that the electronic system is reliably available.
- Auditing: Provides evidence about security-relevant activities, e.g., by keeping logs about certain events.
- Physical security: Provides protection against physical tampering and/or responses to physical tampering attempts.
- Anonymity: Provides protection against discovery and misuse of identity (Paar & Pelzl, 2010).

Digital signatures use asymmetric cryptography. The following figure demonstrates the way that a digital signature works.

Figure 20: How Digital Signatures Work



Source: Docusign, n.d.

The process of digital signing typically consists of three steps. They are

- key generation,
- signing, and
- verification.

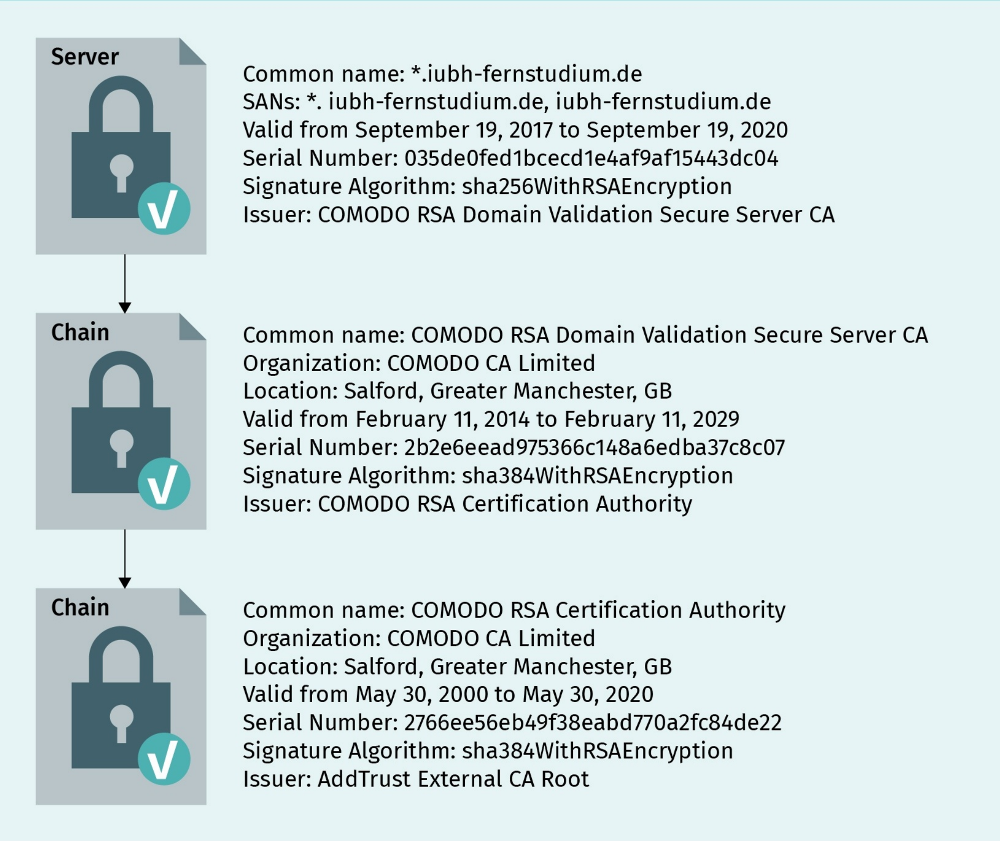
Understanding Public Key Cryptography (PKC) is crucial for better use of the digital signature concept. Public Key Cryptography is relatively new—Whitfield Diffie, Martin Hellman, and Ralph Merkle presented it in 1976. It makes use of asymmetric cryptography with a public and a private key pair. These are public keys, that may be disseminated widely, and private keys, which are known only to the owner. In a PKC system, any person can encrypt a message using the receiver's public key. Messages that have been encrypted this way can only be decrypted with the receiver's private key.

Public Key Infrastructure (PKI) is a centralized function that is used to store and publish public keys as well as other information. It addresses the challenge of exchanging valid public keys. Several implementations exist, for example, a common implementation is Microsoft's Active Directory service. PKI consists of additional services such as the Certificate Authority (CA), a digital certificate, end-user enrollment software, and tools for managing, renewing, and revoking keys and certificates (DocuSign, n.d.).

When a document is signed, we need assurance that the documents and the keys are valid and created securely. Certificate Authorities (CAs) are a type of "trust service provider," which are third party organizations that can provide the necessary digital certificates and have been widely accepted as reliable sources for ensuring key security. Both the entity (the sender of the document) and the recipient must agree to use the same CA. A CA is a company or organization that validates the identities of entities. Entities can be websites, email addresses, companies, individual persons, etc. After validation, CAs bind them to cryptographic keys by issuing electronic documents such as digital certificates (Docusign, n.d.).

A digital certificate is a digital credential that consists of a public key and a block of information that identifies the owner of that certificate. The following figure shows a chain of certificates and how they relate to different CAs in a hierarchy.

Figure 21: Digital Certificate Chain



Common name: *.iubh-fernstudium.de
SANs: *. iubh-fernstudium.de, iubh-fernstudium.de
Valid from September 19, 2017 to September 19, 2020
Serial Number: 035de0fed1bcecd1e4af9af15443dc04
Signature Algorithm: sha256WithRSAEncryption
Issuer: COMODO RSA Domain Validation Secure Server CA

Common name: COMODO RSA Domain Validation Secure Server CA
Organization: COMODO CA Limited
Location: Salford, Greater Manchester, GB
Valid from February 11, 2014 to February 11, 2029
Serial Number: 2b2e6eead975366c148a6edba37c8c07
Signature Algorithm: sha384WithRSAEncryption
Issuer: COMODO RSA Certification Authority

Common name: COMODO RSA Certification Authority
Organization: COMODO CA Limited
Location: Salford, Greater Manchester, GB
Valid from May 30, 2000 to May 30, 2020
Serial Number: 2766ee56eb49f38eabd770a2fc84de22
Signature Algorithm: sha384WithRSAEncryption
Issuer: AddTrust External CA Root

Source: Created on behalf of IU (2020).

Further services in a PKI include the registration authority (RA) that operates alongside a CA to accept requests for new certificates. It verifies the authenticity of a requestor and, when satisfied with the provided documents, issues a digital certificate. A certificate revocation list (CRL) is an electronic list of digital certificates that have been revoked prior to their expiration date. This might be the case if a private key was stolen, a certificate was issued in error, or for another reason.

Another concept that implements digital signatures without a PKI is **PGP**, or Pretty Good Privacy, which was originally described by Phil Zimmerman in 1991. PGP is an encryption program that is used to achieve privacy and authentication. Its functions include signing, encryption, and decryption of text, files, emails, etc. A PGP user maintains a local keyring of all their known and trusted public keys (without CAs). The user makes their own judge-

PGP
This stands for Pretty Good Privacy and does not need CAs but relies on the web of trust.

ment about the trustworthiness of a key using what is called a “web of trust.” A web of trust is when two people who trust each other meet and share their public keys with each other. They also trust the keys that the other persons trusts; hence a web of trust is established (Cole et al., 2005).

PGP can be used to sign or encrypt email messages with a mere click of the mouse. Depending on the version of PGP, the software uses SHA or MD5 to calculate the message hash; CAST, Triple-DES, or IDEA for encryption; and RSA or DSS/Diffie-Hellman for key exchange and digital signatures (Kessler, 2020).

Due to concerns about licensing and patents, a new, free version of PGP emerged, which is available through the International PGP Page and the OpenPGP Alliance (described in RFC 4880). The open-source programming project has developed GnuPG. PGP (or GPG) requires the combination of two encryption/decryption keys—public and private—so that it can work. The public key is always shared with others. The sender uses a public key to encrypt the message. The message is sent, but no one can decipher it, even if they are trying to read the message. The only person that can decrypt the message is the receiver that owns the private key.

7.2 Secure Internet Protocols

Internet is free, easy to use, and is part of our life. To help to protect our data, which are sent thought internet channels, different protocols are required. These protocols can be used for file transfer, email communication, financial transactions, and more. Protocols such as HTTPS, SFTP, SSH, IPSec, SSL, and TLS are part of many applications that we use every day. Network security protocols are designed to prevent unauthorized access to any data that is sent through a network.

Secure Internet Protocols
They are used daily and almost all traffic on modern networks is encrypted using them.

Secure Internet Protocols implement cryptography and encryption techniques to secure the data, meaning that encrypted data can only be decrypted with a special algorithm, mathematical formula, logical key, or a combination of all of them. Internet Protocol Security (IPSec) is an open standard for ensuring private and secure communications over IP networks using cryptographic security services. IPSec-based encryption schemes provide many different security features, including

- confidentiality,
- authentication,
- data integrity, and
- protection against data reply attacks (Cole et al., 2005).

IPSec operates in tunnelled or transport mode. In transport mode, the entire IP packet (the header and data fields) is not encapsulated, but appropriate changes are made to the protocol fields to represent it as a transport mode IPSec packet. Hosts have software directly installed on them so that they can handle transport mode IPSec packets. In tunnelled mode, complete encapsulation of the IP packet takes place in the data field of the IPSec packet. The routers and gateways are normally involved in handling and processing the IPSec packets in the transport mode, but tunnelled mode can address destinations that may not be intended at the source, providing additional security by concealing the source and destination field.

IPSec consists of two main protocols: Encapsulating Security Payload (ESP) and Authentication Header (AH). If ESP is used, then all encapsulated traffic is encrypted. If AH is used, then only IPSec's authentication feature is used.

IPSec can be used to provide secure encrypted communication between two hosts instead of a Secure Internet Protocol network. It can also be used in virtual private networks (VPNs).

Cryptographic algorithms that can be used with IPSec include

- HMAC-SHA1/SHA2 for integrity protection and authenticity.
- TripleDES-CBC for confidentiality.
- AES-CBC for confidentiality.
- AES-GCM for both confidentiality and authentication.
- ChaCha20 + Poly1305 for both confidentiality and authentication. IPSec uses cryptographic security services.

Hypertext Transfer Protocol Secure (HTTPS) is a protocol that protects the integrity and confidentiality of data between a user's computer and a site. Data sent using HTTPS are secured via **Transport Layer Security** (TLS) protocol connection.

Transport Layer Security
TLS works on top of the TCP layer in the TCP/IP protocol stack.

The TLS's basic aim is to provide authentication and integrity negotiation between applications involved. The negotiations can be used to decide which encryption algorithms will be used in the data exchange between the two parties. Today, most of the Web browsers, such as Chrome and Firefox, come with built-in TLS support that make them relatively transparent to the end user (Cole et al., 2005). **Secure Sockets Layer** (SSL) (and its successor Transport Layer Security (TLS)) is an encryption protocol that is used to establish an encrypted link between nodes—typically a Web server (website) and a browser, or a mail server and an email client.

Secure Sockets Layer
SSL is an old version of TLS.

TLS relies on public key cryptography for mutual authentication, confidentiality, and data integrity for Web browsers. The system provides high-end security for the Web browsers at very little incremental cost. Most transactions require protection between the servers and the clients. The servers require the verification of the user when remote users download proprietary and confidential information from an organization's server. There are three versions of the SSL protocol, but the first version was never released. All of these SSL versions are now obsolete and have been replaced with TLS. At the time of writing, the current version is TLS 1.3, and only TLS version 1.2 and above are deemed to be secure.

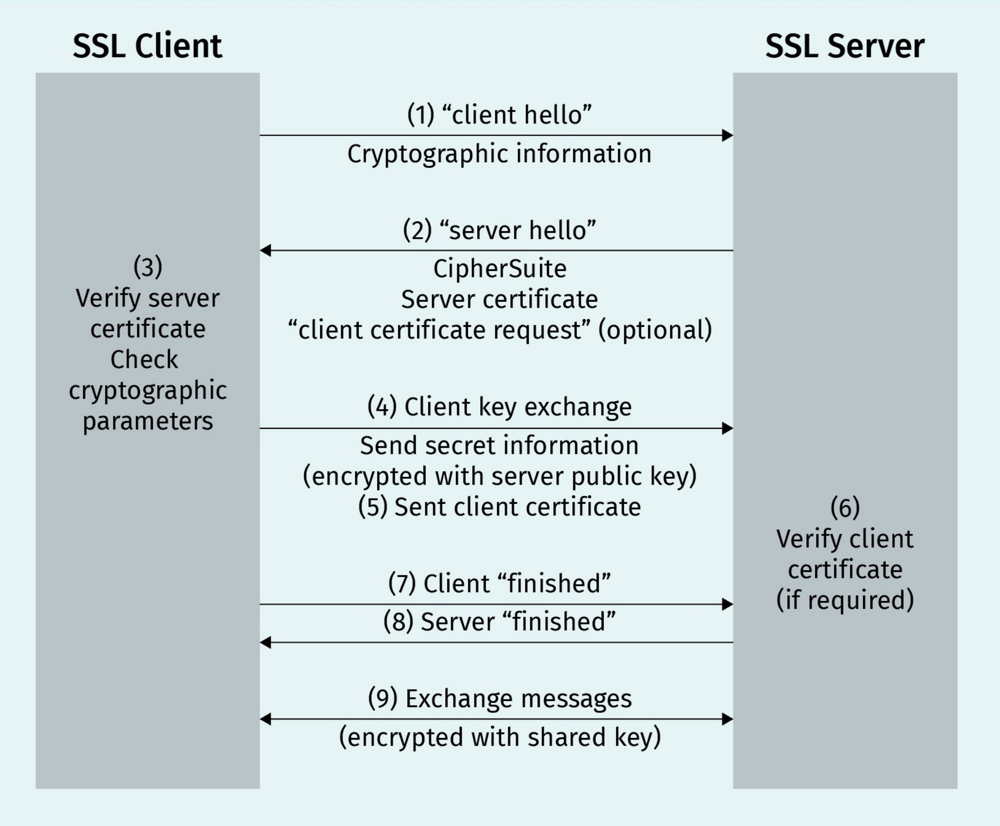
When installed on a (Web) server, TLS certificates (small data files that bind a cryptographic key to an organization) activate the HTTPS protocol. This allows secure connections from a Web server to a browser. TLS is not only used to secure credit card transactions, data transfer, and logins, but it is now the norm when securing the browsing of all sorts of sites. This certificate needs to be installed on the server to initiate a secure session with the Web browser. After the connection has been successfully established, all Web traffic will be secured through HTTPS protocol. This means that after installing a certificate on a server, HTTP will be automatically changed to HTTPS.

The three main components of TLS are

- encryption (hides the transferred data from others),
- authentication (ensures that the sides who exchange information are who they claim to be), and
- integrity (verifies that the data has not been forged or tampered with) (Cloudflare, n.d.).

TLS protocol encrypts internet traffic of all types. The SSL or TLS handshake enables the SSL or TLS client and server to establish the secret keys with which they communicate. The TLS handshake is a process that consists of multiple steps. A basic TLS handshake involves the client and server sending "hello" messages and the exchange of keys, a cipher message, and a finish message. The multi-step process is what makes TLS flexible enough to use in different applications because the format and order of exchange can be modified (Dierks & Rescola, 2008).

Figure 22: TLS/SSL Handshake



Source: IBM, 2020.

TLS uses a hybrid form of cryptography. The connection is established using asymmetric cryptography. This connection is used to exchange the key that is then used to encrypt the connection symmetrically, since asymmetric cryptography is very costly and slow compared to symmetric cryptography.

7.3 Blockchain

A **blockchain** is a growing list of records, called blocks. The blocks are linked together using cryptography. They are usually implemented as Merkle trees. Hashing is used to identify the previous block; hence, each subsequent block includes the hash of the previous block, a timestamp, and data. A blockchain is setup as a peer-to-peer network and is resistant against manipulations. Compared to a classic database, the record-keeping on a blockchain is decentralized, making it almost impossible to destroy the integrity of records in the blockchain.

Blockchain
Based on P2P and public electronic ledger, blockchain is used to let people share data securely and without tampering.

Nodes share data in a secure, tamper-proof way, even without the need to trust each other. Blockchain makes this possible because it stores data using cryptography rules that are extremely difficult for attackers to manipulate (Orcutt, 2018). However, it comes with a cost—blockchain databases are more costly to maintain than central databases, such as relational database systems.

Blockchain technology is based on a peer-to-peer (P2P) network topology and a "public electronic ledger." Blockchain technology allows data to be stored globally on any device. Anyone in this network can see everyone else's entries in real time. This function of blockchain allows users to create an "unchangeable" record of transactions. Every transaction is time-stamped and linked to the previous one in a chain. When a new set of transactions is added, the data becomes another block in the chain, hence the name blockchain. Every transaction on a blockchain is secured with a digital signature, meaning that authenticity can be proved. Using encryption and digital signatures, the data stored on the blockchain cannot be changed and is therefore immutable.

A result of the open structure of the blockchain is that anonymity cannot be achieved but the data is pseudonymized only. Also, data that was once accepted to the blockchain stays there forever. This might have legal implications in the future as it will be difficult to achieve privacy. A situation might evolve where illegal content is stored on the blockchain that cannot be removed by anyone.

Typical blockchains use elliptic-curve-cryptography (ECC) to sign the blocks. Each block in a blockchain network stores some information within the hash of its previous block. This hash is a unique code of a specific block. If we change or modify the information inside the block, the hash of the block will also be modified. Unique hash keys that connect the blocks are the reason that blockchain is secure.

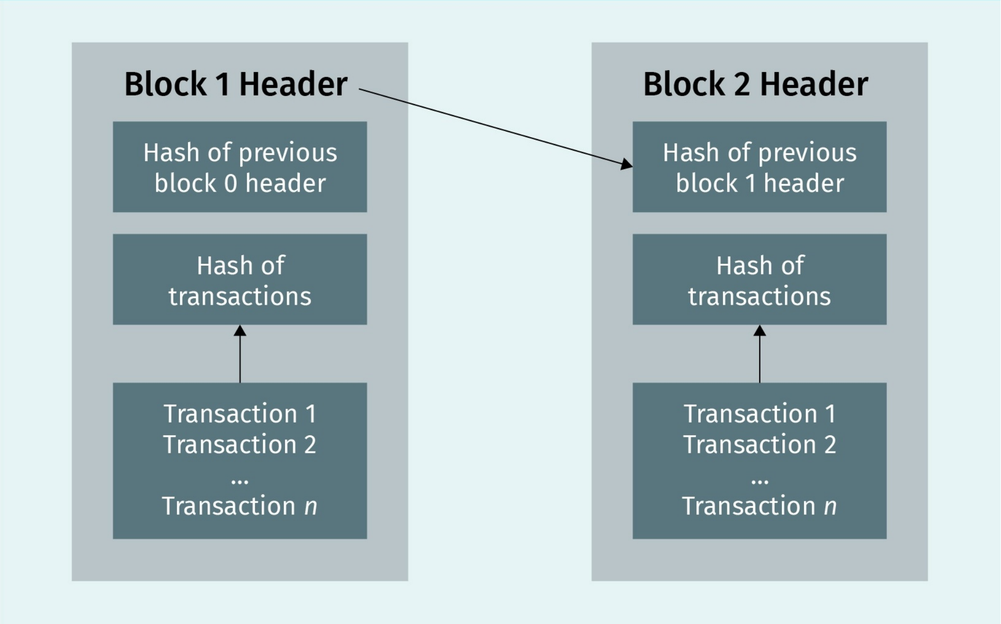
Blockchain can be classified as either public or private. In a public blockchain, the ledger is public and can be accessed by anyone who has access to the network in the form of an internet connection. Private blockchains, however, are only shared among the trusted participants, for example, within a company. There are four main features that characterize blockchain and will determine the future use of this technology.

- Immutable—The data cannot be changed and therefore has integrity.
- Tamper-proof—Data tampering is prevented, but if it occurs, it is detected, as mechanisms exist to cope with tampering.
- Decentralization—Nobody owns the network; it is owned by all entities that participate and hold a copy of the current blockchain.
- Peer-to-peer network—There is no central server, meaning that all peers in the network are equal.

Blockchain technology has many uses outside of cryptocurrency. There are a lot of domains where it is currently used or will be used in the future. These include supply chain communications, distributed storage, digital voting, smart contracts as legal documents, process of digitalization, and more. Typical open source implementations can be found at the Hyperledger project, administered by the Linux Foundation (The Linux Foundation, n.d.). Hyperledger is often used in private blockchains, and several cloud computing providers offer it as part of their services.

The figure below shows a simplified blockchain.

Figure 23: Blockchain Schema



Source: Created on behalf of IU (2020).

7.4 Electronic Money

According to some sources, electronic money (“e-money”, digital currency, digital money, or electronic currency) is broadly defined as an “electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer” (European Central Bank, n.d., Electronic Money Section, para. 1). E-money products can be hardware-based (e.g., chip cards) or software-based (specialized software such as PayPal that is installed on smartphones, tablets, and PCs), depending on the technology used to store the monetary value. E-money can either be centralized with the control point, or decentralized without the control point, meaning that it can come from various sources or networks of sources such as virtual values or Bitcoin.

There are two main challenges that electronic money needs to address.

1. Privacy: In contrast to physical coins and bills, electronic money exists in a database and it contains information concerning who transferred money to whom, the amount, and potentially even for which services the transaction was executed.
2. Double spend: An electronic system could be tampered with so that a double spend might be enacted by fraudsters or just by mistake. This would lead to inflation and mistrust into the electronic money system.

The idea of digital cash was introduced for the first time in the research of Chaum, published in 1982. In short, electronic money (e-money) is the money balance recorded electronically on a stored-value card or remotely on a server. The Bank for International Settlements (1997, pp. 2—3), which is a Central Bank Cooperation based in Basel, Switzerland, defines e-money as “stored-value or prepaid payment mechanisms for executing payments via point-of-sale terminals, direct transfers between two devices, or even open computer networks such as the internet.” Some say that examples of e-money are bank deposits, electronic fund transfers, payment processors, and digital currencies. It could be said that all transactions and money keeping where computer systems, data storage systems, and computer networks are involved can be defined as e-money.

There are several kinds of e-money in use and currently in development. Credit cards can be used both offline and in e-commerce. PCI DSS sets stringent rules for this method of payment. If used online, it usually uses TLS to encrypt the connection. Authentication methods vary but include a second factor such as Verified by Visa or 3DSecure of MasterCard. Bank transfers are another method to transfer money. They can also be used so that providers get direct access to a user’s bank account and execute the transfer so that the recipient has confidence that the transfer took place. Mobile money wallets are often used by those who do not have access to classical banking or credit cards. Their security is mainly based on keys and certificates on the SIM card and secure SMS. A layer above bank accounts or credit cards are online payment providers such as AliPay or PayPal. These services rely on this basic payment infrastructure, but add a layer of comfort. These apps only require the scan of a QR code or an email address to perform a transaction. Security relies on TLS and MFA for authentication. Digital certificates and signatures ensure non-repudiation.

The development of cryptocurrency is the newest stage of money evolution (Vlasov, 2017). According to Investopedia, “a cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double spend” (Frankenfield, 2020, What Is... Section, para. 1).

Bitcoin
This and other cryptocurrencies were created answering the 2008 financial crisis.

The first widely adopted blockchain-based cryptocurrency, which can also be classed as decentralized e-money, is **Bitcoin**. It remains the most popular cryptocurrency and has the highest market capitalization of all cryptocurrencies at the time of writing. Bitcoin is an electronic money system, established in 2009. It is a free and innovative platform—anyone is free to program and run services on the open Bitcoin standard as there are no required permissions from central authorities. Bitcoin is a very popular cryptocurrency because, firstly, the banks and the government do not control it, and secondly, people can spend their Bitcoins anonymously. Bitcoins can be purchased and payed for with fiat currency, or it can be mined using computing power. After you have installed a Bitcoin wallet (to store private keys of bitcoins) on an electronic device, a first Bitcoin address will be generated. After that, more and more Bitcoin addresses can be created. These addresses can be sent to another person to send or receive money. Bitcoin addresses should only be used once.

Every Bitcoin transaction is recorded in a public list called a blockchain. Blockchain is an essential component of many cryptocurrencies. Today, most cryptocurrencies use blockchain technology to record transactions. Although all transactions are recorded, there is no account number to identify a person—blockchain preserves anonymity. The decentralized nature of Bitcoin may make it more expensive and more difficult to market new services, as they are likely to be pitched directly to users rather than to a small set of intermediaries. Innovators without much marketing experience may be unable to sustain their innovations (Nian & Chuen, 2015).

Transactions are signed using asymmetric cryptography based on elliptic-curve cryptography (ECC). The mining of bitcoin involves finding a SHA-256 hash for the next block, this is called “proof of work.” As this is energy-intensive and provides no further value, other cryptocurrencies use some other concepts such as “proof of stake.” In a proof of stake process, the holder of most units of a cryptocurrency gets the reward for approving the next transaction (instead of the one who invested the most computing power). Some studies state that the evolution of electronic money has led to cryptocurrency having significant advantages over other forms of money (Vlasov, 2017).

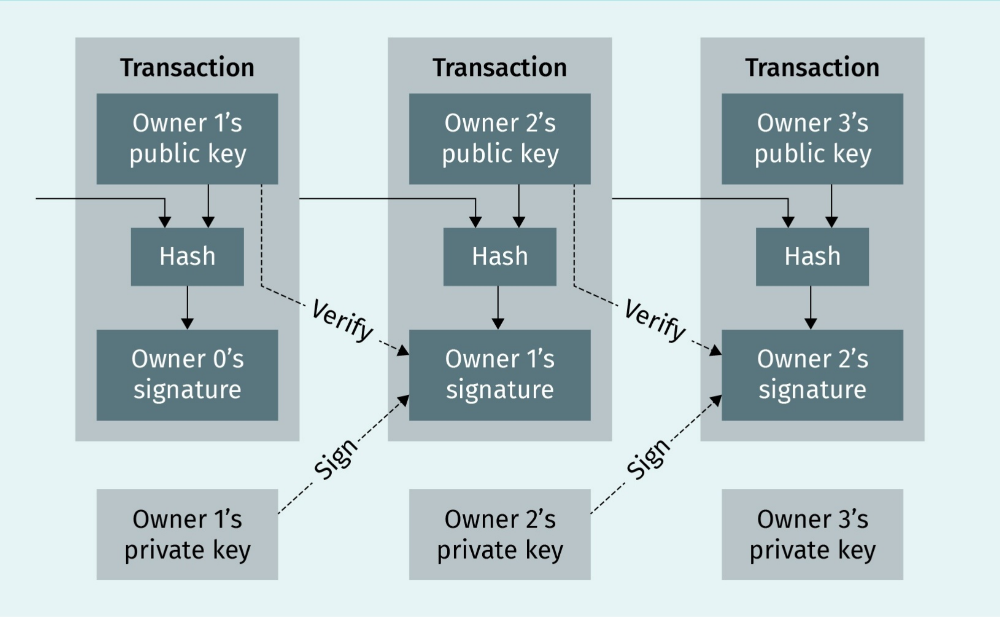
The cryptocurrency system must meet a few conditions (Lansky, 2018).

- The system must have distributed consensus so there is no need for a central authority.
- The system must keep an overview of cryptocurrency units and their ownership.
- The system must define whether new cryptocurrency units can be created. If yes, the system defines how to determine the ownership of these and the circumstances of their origin.
- Ownership of cryptocurrency units can only be proved by using cryptography.
- The system must allow transactions in which ownership of the cryptographic units is changed.

- If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system must only perform one of them.

The following figure shows transactions on the Bitcoin blockchain.

Figure 24: Transactions on the Bitcoin Blockchain



Source: Nakamoto, 2008.

SUMMARY

In this unit, the concepts and possibilities of applied cryptography have been explored. The benefits of digital signatures and Public Key Cryptography were discussed in detail with emphasis on the ways they can provide security. Blockchain, or distributed ledger technology, and its applications were also covered, focusing on the ways that blockchain can ensure the authenticity and integrity of data.