The Art of Protecting Secrets

16 January 2024 22:49

The principles of cryptology explain how modern day protocols and algorithms secure communications. Cryptology is the science of making and breaking secret codes. The development and use of codes is cryptography. Studying and breaking codes is cryptanalysis. Society has used cryptography for centuries to protect secret documents. For example, Julius Caesar used a simple alphabetic cipher to encrypt messages to his generals in the field. His generals would have knowledge of the cipher key required to decrypt the messages. Today, modern day cryptographic methods ensure secure communications.
Access control is, as its name suggests, a way of controlling access to a building, a room, a system, a database, a file, and information. Organizations employ a variety of access control techniques to protect confidentiality. This chapter will examine the four steps in the access control process: 1) identification, 2) authentication, 3) authorization, and 4) accountability. In addition, the chapter describes the different access control models and access control type

What is Cryptography?

Cryptology is the science of making and breaking secret codes. Cryptography is a way to store and transmit data so only the intended recipient can read or process it. Modern cryptography uses computationally secure algorithms to make sure that cyber criminals cannot easily compromise protected information.
Data confidentiality ensures privacy so that only the intended receiver can read the message. Parties achieve this through encryption. Encryption is the process of scrambling data so that an unauthorized party cannot easily read it.
When enabling encryption, readable data is plaintext, or cleartext, while the encrypted version is encrypted text or ciphertext. Encryption converts the plaintext readable message to ciphertext, which is the unreadable, disguised message. Decryption reverses the process. Encryption also requires a key, which plays a critical role in encrypting and decrypting a message. The person possessing the key can decrypt the ciphertext to plaintext.
Historically, parties have used various encryption algorithms and methods. An algorithm is the process or formula used to solve a problem. Julius Caesar is said to have secured messages by putting two sets of the alphabet, side-by-side, and then shifting one of them by a specific number of places. The number of places in the shift serves as the key. He converted plaintext into ciphertext using this key, and only his generals, who also had the key, knew how to decipher the messages. This method is the Caesar cipher. The figure shows a secret message using the Caesar cipher.

Creating Ciphertext

Each encryption method uses a specific algorithm, called a cipher, to encrypt and decrypt messages. A cipher is a series of well-defined steps used to encrypt and decrypt messages. There are several methods of creating ciphertext:

- Transposition – letters are rearranged (Figure 1)
- Substitution – letters are replaced (Figure 2)
- One-time pad – plaintext combined with a secret key creates a new character, which then combines with the plaintext to produce ciphertext (Figure 3)

Old encryption algorithms, such as the Caesar cipher or the Enigma machine, depended on the secrecy of the algorithm to achieve confidentiality. With modern technology, where reverse engineering is often simple, parties use public-domain algorithms. With most modern algorithms, successful decryption requires knowledge of the appropriate cryptographic keys. This means that the security of encryption lies in the secrecy of the keys, not the algorithm.
Some modern encryption algorithms still use transposition as part of the algorithm.
Key management is the most difficult part of designing a cryptosystem. Many cryptosystems have failed because of mistakes in their key management, and all modern cryptographic algorithms require key management procedures. In practice, most attacks on cryptographic systems involve attacking the key management system, rather than the cryptographic algorithm itself.

Two Types of Encryption

Cryptographic encryption can provide confidentiality by incorporating various tools and protocols.
There are two approaches to ensuring the security of data when using encryption. The first is to protect the algorithm. If the security of an encryption system depends on the secrecy of the algorithm itself, the most important aspect is to guard the algorithm at all costs. Every time someone finds out the details of the algorithm, every party involved would need to change the algorithm. That approach does not sound very secure or manageable. The second approach is to protect the keys. With modern cryptography, the algorithms are public. The cryptographic keys ensure the secrecy of the data. Cryptographic keys are

passwords that are part of the input into an encryption algorithm together along with the data requiring encryption.
There are two classes of encryption algorithms:
Symmetric algorithms - These algorithms use the same pre-shared key, sometimes called a secret key pair, to encrypt and decrypt data. Both the sender and receiver know the pre-shared key before any encrypted communication begins. As shown in Figure 1, symmetric algorithms use the same key to encrypt and decrypt the plaintext. Encryption algorithms that use a common key are simpler and need less computational power.
Asymmetric algorithms - Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key, as shown in Figure 2. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute.

The Symmetrical Encryption Process

Symmetric algorithms use the same pre-shared key to encrypt and decrypt data, a method also known as private-key encryption.
For example, Alice and Bob live in different locations and want to exchange secret messages with one another through the mail system. Alice wants to send a secret message to Bob.
Private-key encryption uses a symmetric algorithm. As illustrated by the keys in the figure, Alice and Bob have identical keys to a single padlock. The key exchange happened prior to sending any secret messages. Alice writes a secret message and puts it in a small box that she locks using the padlock. She mails the box to Bob. The message is safe inside the box as the box makes its way through the post office system. When Bob receives the box, he uses his key to unlock the padlock and retrieve the message. Bob can use the same box and padlock to send a secret reply back to Alice.
If Bob wants to talk to Carol, he needs a new pre-shared key for that communication to keep it secret from Alice. The more people Bob wants to communicate with securely, the more keys he will need to manage.

Types of Cryptography

The most common types of cryptography are block ciphers and stream ciphers. Each method differs in the way that it groups bits of data to encrypt it.
Block Ciphers
Block ciphers transform a fixed-length block of plaintext into a common block of ciphertext of 64 or 128 bits. Block size is the amount of data encrypted at any one time. To decrypt this ciphertext, apply the reverse transformation to the ciphertext block, using the same secret key.
Block ciphers usually result in output data that is larger than the input data, because the ciphertext must be a multiple of the block size. For example, Data Encryption Standard (DES) is a symmetric algorithm that encrypts blocks in 64-bit chunks using a 56-bit key. To accomplish this, the block algorithm takes data one chunk at a time, for example, 8 bytes per chunk, until the entire block is full. If there is less input data than one full block, the algorithm adds artificial data, or blanks, until it uses the full 64 bits, as shown in Figure 1 for the 64 bits on the left.
Stream Ciphers
Unlike block ciphers, stream ciphers encrypt plaintext one byte or one bit at a time, as shown in Figure 2. Think of stream ciphers as a block cipher with a block size of one bit. With a stream cipher, the transformation of these smaller plaintext units varies, depending on when they are encountered during the encryption process. Stream ciphers can be much faster than block ciphers, and generally do not increase the message size, because they can encrypt an arbitrary number of bits.
A5 is a stream cipher that provides voice privacy and encrypts cell phone communications. It is also possible to use DES in stream cipher mode.
Complex cryptographic systems can combine block and stream in the same process.

Symmetric Encryption Algorithms

Numerous encryption systems use symmetric encryption. Some of the common encryption standards that use symmetric encryption include the following:
3DES (Triple DES): Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses a 56-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext. It always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. A permutation is a way of arranging all elements of a set.
Triple DES encrypts data three times and uses a different key for at least one of the three passes, giving it a cumulative key size of 112-168 bits. 3DES is resistant to attack, but it is much slower than DES.
The 3DES encryption cycle is as follows:
1. Data encrypted by first DES
2. Data decrypted by second DES
3. Data re-encrypted by third DES
The reverse process decrypts the ciphertext.
IDEA: The International Data Encryption Algorithm (IDEA) uses 64-bit blocks and 128-bit keys. IDEA performs eight rounds of transformations on each of the 16 blocks that results from dividing each 64-bit

block. IDEA was the replacement for DES, and now PGP (Pretty Good Privacy) uses it. PGP is a program that provides privacy and authentication for data communication. GNU Privacy Guard (GPG) is a licensed, free version of PGP.
AES: The Advanced Encryption Standard (AES) has a fixed block size of 128-bits with a key size of 128, 192, or 256 bits. The National Institute of Standards and Technology (NIST) approved the AES algorithm in December 2001. The U.S. government uses AES to protect classified information.
AES is a strong algorithm that uses longer key lengths. AES is faster than DES and 3DES, so it provides both a solution for software applications as well as hardware use in firewalls and routers.
Other block ciphers include Skipjack (developed by the NSA), Blowfish, and Twofish.

The Asymmetrical Encryption Process

Asymmetric encryption, also called public-key encryption, uses one key for encryption that is different from the key used for decryption. A criminal cannot calculate the decryption key based on knowledge of the encryption key, and vice versa, in any reasonable amount of time.
If Alice and Bob exchange a secret message using public-key encryption, they use an asymmetric algorithm. This time Bob and Alice do not exchange keys prior to sending secret messages. Instead, Bob and Alice each have a separate padlock with separate corresponding keys. For Alice to send a secret message to Bob, she must first contact him and ask him to send his open padlock to her. Bob sends the padlock but keeps his key. When Alice receives the padlock, she writes her secret message and puts it in a small box. She also puts her open padlock in the box but keeps her key. She then locks the box with Bob's padlock. When Alice locks the box, she is no longer able to get inside because she does not have a key to that padlock. She mails the box to Bob and, as the box travels through the mail system, no one is able to open it. When Bob receives the box, he can use his key to unlock the box and retrieve the message from Alice. To send a secure reply, Bob puts his secret message in the box, along with his open padlock, and locks the box using Alice's padlock. Bob mails the secured box back to Alice.
For example, in Figure 1, Alice requests and obtains Bob's public key. In Figure 2, Alice uses Bob's public key to encrypt a message using an agreed-upon algorithm. Alice sends the encrypted message to Bob, and Bob then uses his private key to decrypt the message, as shown in Figure 3.

Asymmetric Encryption Algorithms

Asymmetric algorithms use formulas that anyone can look up. The pair of unrelated keys is what makes these algorithms secure. The asymmetric algorithms include:
RSA (Rivest-Shamir-Adleman) - uses the product of two very large prime numbers with an equal length of between 100 and 200 digits. Browsers use RSA to establish a secure connection.
Diffie-Hellman - provides an electronic exchange method to share the secret key. Secure protocols, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), and Internet Protocol Security (IPsec), use Diffie-Hellman.
ElGamal - uses the U.S. government standard for digital signatures. This algorithm is free for use because no one holds the patent.
Elliptic Curve Cryptography (ECC) - uses elliptic curves as part of the algorithm. In the U.S., the National Security Agency uses ECC for digital signature generation and key exchange.

Key Management

Key management includes the generation, exchange, storage, use, and replacement of keys used in an encryption algorithm.
Key management is the most difficult part of designing a cryptosystem. Many cryptosystems have failed because of mistakes in their key management procedures. In practice, most attacks on cryptographic systems target the key management level, rather than the cryptographic algorithm itself.
As shown in the figure, there are several essential characteristics of key management to consider.
Two terms used to describe keys are:

- **Key length** - Also called the key size, this is the measure in bits.
- **Keyspace** - This is the number of possibilities that a specific key length can generate.

As key length increase, the keyspace increases exponentially. The keyspace of an algorithm is the set of all possible key values. Longer keys are more secure; however, they are also more resource intensive. Almost every algorithm has some weak keys in its keyspace that enable a criminal to break the encryption via a shortcut.

Comparing Encryption Types

It is important to understand the differences between symmetric and asymmetric encryption methods. Symmetric encryption systems are more efficient and can handle more data. However, key management with symmetric encryption systems is more problematic and harder to manage. Asymmetric cryptography is more efficient at protecting the confidentiality of small amounts of data, and its size and speed make it more secure for tasks such as electronic key exchange which is a small amount of data rather than encrypting large blocks of data.
Maintaining confidentiality is important for both data at rest and data in motion. In both cases, symmetric encryption is favored because of its speed and the simplicity of the algorithm. Some asymmetric algorithms

can significantly increase the size of the object encrypted. Therefore, in the case of data in motion, use public key cryptography to exchange the secret key, and then symmetric cryptography to ensure the confidentiality of the data sent.

Applications

There are many applications for both symmetric and asymmetric algorithms.
A one-time password-generating token is a hardware device that uses cryptography to generate a one-time password. A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for one transaction of one session only. The number changes every 30 seconds or so. The session password appears on a display and the user enters the password.
The electronic payment industry uses 3DES. Operating systems use DES to protect user files and system data with passwords. Most encrypting file systems, such as NTFS, use AES.
Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE), which is a fundamental component of IPsec Virtual Private Networks (VPNs).
- Secure Socket Layer (SSL), which is a means of implementing cryptography into a web browser.
- Secure Shell (SSH), which is a protocol that provides a secure remote access connection to network devices.
- Pretty Good Privacy (PGP), which is a computer program that provides cryptographic privacy and authentication to increase the security of email communications.

A VPN is a private network that uses a public network, usually the Internet, to create a secure communication channel. A VPN connects two endpoints such as two remote offices over the Internet to form the connection.
VPNs use IPsec. IPsec is a suite of protocols developed to achieve secure services over networks. IPsec services allow for authentication, integrity, access control, and confidentiality. With IPsec, remote sites can exchange encrypted and verified information.
Data in use is a growing concern to many organizations. When in use, data no longer has any protection because the user needs to open and change the data. System memory holds data in use and it can contain sensitive data such as the encryption key. If criminals compromise data in use, they will have access to data at rest and data in motion.

Physical Access Controls

Physical access controls are actual barriers deployed to prevent direct contact with systems. The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets.
Physical access control determines who can enter (or exit), where they can enter (or exit), and when they can enter (or exit).
Examples of physical access controls include the following:

- Guards (Figure 1) monitor the facility
- Fences (Figure 2) protect the perimeter
- Motion detectors (Figure 3) detect moving objects
- Laptop locks (Figure 4) safeguard portable equipment
- Locked doors (Figure 5) prevent unauthorized access
- Swipe cards (Figure 6) allow access to restricted areas
- Guard dogs (Figure 7) protect the facility
- Video cameras (Figure 8) monitor a facility by collecting and recording images
- Mantraps (Figure 9) allow access to the secured area after door 1 closes
- Alarms (Figure 10) detect intrusion

Logical Access Controls

Logical access controls are the hardware and software solutions used to manage access to resources and systems. These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.
Logical access controls include the following:

- Encryption is the process of taking plaintext and creating ciphertext
- Smart cards have an embedded microchip
- Passwords are protected string of characters
- Biometrics are users' physical characteristics
- Access Control Lists (ACLs) define the type of traffic allowed on a network
- Protocols are a set of rules that govern the exchange of data between devices
- Firewalls prevent unwanted network traffic
- Routers connect at least two networks

- Intrusion Detection Systems monitor a network for suspicious activities
- Clipping Levels are certain allowed thresholds for errors before triggering a red flag

Administrative Access Controls

Administrative access controls are the policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access. Administrative controls focus on personnel and business practices. Administrative controls include the following:

- Policies are statements of intent
- Procedures are the detailed steps required to perform an activity
- Hiring practices involves the steps an organization takes to find qualified employees
- Background checks are an employment screening that includes information of past employment verification, credit history, and criminal history
- Data classification categorizes data based on its sensitivity
- Security training educates employees about the security policies at an organization
- Reviews evaluate an employee's job performance

Mandatory Access Control

Mandatory access control (MAC) restricts the actions that a subject can perform on an object. A subject can be a user or a process. An object can be a file, a port, or an input/output device. An authorization rule enforces whether or not a subject can access the object.
Organizations use MAC where different levels of security classifications exist. Every object has a label and every subject has a clearance. A MAC system restricts a subject based on the security classification of the object and the label attached to the user.
For example, take the military security classifications Secret and Top Secret. If a file (an object) is considered top secret, it is classified (labeled) Top Secret. The only people (subjects) that may view the file (object) are those with a Top Secret clearance. It is up to the access control mechanism to ensure that an individual (subject) with only a Secret clearance, never gains access to a file labeled as Top Secret.
Similarly, a user (subject) cleared for Top Secret access cannot change the classification of a file (object) labeled Top Secret to Secret. Additionally, a Top Secret user cannot send a Top Secret file to a user cleared only to see Secret information.

Discretionary Access Control

An object's owner determines whether to allow access to an object with discretionary access control (DAC). DAC grants or restricts object access determined by the object's owner. As the name implies, controls are discretionary because an object owner with certain access permissions can pass on those permissions to another subject.
In systems that employ discretionary access controls, the owner of an object can decide which subjects can access that object and what specific access they may have. One common method to accomplish this is with permissions, as shown in the figure. The owner of a file can specify what permissions (read/write/execute) other users may have.
Access control lists are another common mechanism used to implement discretionary access control. An access control list uses rules to determine what traffic can enter or exit a network

Role-Based Access Control

Role-based access control (RBAC) depends on the role of the subject. Roles are job functions within an organization. Specific roles require permissions to perform certain operations. Users acquire permissions through their role.
RBAC can work in combination with DAC or MAC by enforcing the policies of either one. RBAC helps to implement security administration in large organizations with hundreds of users and thousands of possible permissions. Organizations widely accept the use of RBAC to manage computer permissions within a system, or application, as a best practice.

Rule-Based Access Control

Rule-based access control uses access control lists (ACLs) to help determine whether to grant access. A series of rules is contained in the ACL, as shown in the figure. The determination of whether to grant access depends on these rules. An example of such a rule is one that states that no employee may have access to the payroll file after hours or on weekends.
As with MAC, users cannot change the access rules. Organizations can combine rule-based access control with other strategies for implementing access restrictions. For example, MAC methods can utilize a rule-based approach for implementation.

What is Identification?

Identification enforces the rules established by the authorization policy. A subject requests access to a system resource. Every time the subject requests access to a resource, the access controls determine whether to grant or deny access. For example, the authorization policy determines what activities a user can perform on a resource.
A unique identifier ensures the proper association between allowed activities and subjects. A username is the most common method used to identify a user. A username can be an alphanumeric combination, a personal identification number (PIN), a smart card, or biometric, such as a fingerprint, retina scan, or voice recognition.
A unique identifier ensures that a system can identify each user individually; therefore, allowing an authorized user to perform the appropriate actions on a particular resource.

What You Know

Passwords, passphrases, or PINs are all examples of something that the user knows. Passwords are the most popular method used for authentication. The terms passphrase, passcode, passkey, or PIN are generically referred to as password. A password is a string of characters used to prove a user's identity. If this string of characters relates back to a user (such as a name, birthdate, or address), it will be easier for cyber criminals to guess a user's password.
A number of publications recommend that a password be at least eight characters. Users should not create a password that is so long that it is difficult to memorize, or conversely, so short that it becomes vulnerable to password cracking. Passwords should contain a combination of upper and lowercase letters, numbers, and special characters. Click here to test current passwords.
Users need to use different passwords for different systems because if a criminal cracks the user's password once, the criminal will have access to all of a user's accounts. A password manager can help a user create and remember strong passwords. Click here to view a strong password generator.

What You Have

Smart cards and security key fobs are both examples of something that users have in their possession.
Smart Card Security (Figure 1) – A smart card is a small plastic card, about the size of a credit card, with a small chip embedded in it. The chip is an intelligent data carrier, capable of processing, storing, and safeguarding data. Smart cards store private information, such as bank account numbers, personal identification, medical records, and digital signatures. Smart cards provide authentication and encryption to keep data safe.
Security Key Fob (Figure 2) – A security key fob is a device that is small enough to attach to a key ring. It uses a process called two-factor authentication, which is more secure than a username and password combination. First, the user enters a personal identification number (PIN). If correctly entered, the security key fob will display a number. This is the second factor, which the user must enter to log in to the device or network.

Who You Are

A unique physical characteristic, such as a fingerprint, retina, or voice, that identifies a specific user is called biometrics. Biometric security compares physical characteristics against stored profiles to authenticate users. A profile is a data file containing known characteristics of an individual. The system grants the user access if his or her characteristics match saved settings. A fingerprint reader is a common biometric device.
There are two types of biometric identifiers:

- **Physiological characteristics** – these include fingerprints, DNA, face, hands, retina, or ear features
- **Behavioral characteristics** - include patterns of behavior, such as gestures, voice, typing rhythm, or the way a user walks

Biometrics is becoming increasingly popular in public security systems, consumer electronics, and point-of-sale applications. Implementing biometrics uses a reader or scanning device, software that converts the scanned information into digital form, and a database that stores biometric data for comparison.

Multi-factor Authentication

Multi-factor authentication uses at least two methods of verification. A security key fob is a good example. The two factors are something you know, such as a password, and something you have, such as a security key fob. Take this a step further by adding something you are, such as a fingerprint scan.
Multi-factor authentication can reduce the incidence of online identity theft because knowing the password would not give cyber criminals access to user information. For example, an online banking website might require a password and a PIN that the user receives on his or her smartphone. As shown in the figure, withdrawing cash from an ATM is another example of multifactor authentication. The user must have the bankcard and know the PIN before the ATM will dispense cash.

What is Authorization?

Authorization controls what a user can and cannot do on the network after successful authentication. After a user proves his or her identity, the system checks to see what network resources the user can access and what the user can do with the resources. As shown in the figure, authorization answers the question, "What read, copy, create, and delete privileges does the user have?"

Authorization uses a set of attributes that describes the user's access to the network. The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local router where the user is connected.
Authorization is automatic and does not require users to perform additional steps after authentication. Implement authorization immediately after the user authenticates.

Using Authorization

Defining authorization rules is the first step in controlling access. An authorization policy establishes these rules.
A group membership policy defines authorization based on membership in a specific group. For example, all employees of an organization have a swipe card, which provides access to the facility. If an employee's job does not require that she have access to the server room, her security card will not allow her to enter that room.
An authority-level policy defines access permissions based on an employee's standing within the organization. For example, only senior-level employees in an IT department may access the server room.

What is Accountability?

Accountability traces an action back to a person or process making the change to a system, collects this information, and reports the usage data. The organization can use this data for such purposes as auditing or billing. The collected data might include the log in time for a user, whether the user log in was a success or failure, or what network resources the user accessed. This allows an organization to trace actions, errors, and mistakes during an audit or investigation.

Implementing Accountability

Implementing accountability consists of technologies, policies, procedures, and education. Log files provide detailed information based on the parameters chosen. For example, an organization may look at the log for login failures and successes. Login failures can indicate that a criminal tried to hack an account. Login successes tell an organization which users are using what resources and when. Is it normal for an authorized user to access the corporate network at 3:00 a.m.? The organization's policies and procedures spell out what actions should be recorded and how the log files are generated, reviewed and stored.
Data retention, media disposal, and compliance requirements all provide accountability. Many laws require the implementation of measures to secure different data types. These laws guide an organization on the right way to handle, store, and dispose of data. The education and awareness of an organization's policies, procedures, and related laws can also contribute to accountability.

Preventive Controls

Prevent means to keep something from happening. Preventive access controls stop unwanted or unauthorized activity from happening. For an authorized user, a preventive access control means restrictions. Assigning user specific privileges on a system is an example of a preventive control. Even though a user is an authorized user, the system puts limits in place to prevent the user from accessing and performing unauthorized actions. A firewall that blocks access to a port or service that cyber criminals can exploit is also a preventive control.

Deterrent Controls

A deterrent is the opposite of a reward. A reward encourages individuals to do the right thing, while a deterrent discourages them from doing the wrong thing. Cyber security professionals and organizations use deterrents to limit or mitigate an action or behavior, but deterrents do not stop them. Access control deterrents discourage cyber criminals from gaining unauthorized access to information systems and sensitive data. Access control deterrents discourage attacking systems, stealing data, or spreading malicious code. Organizations use access control deterrents to enforce cybersecurity policies.
Deterrents make potential cyber criminals think twice before committing a crime. The figure lists common access control deterrents used in the cybersecurity world.

Detective Controls

Detection is the act or process of noticing or discovering something. Access control detections identify different types of unauthorized activity. Detection systems can be very simple, such as a motion detector or security guard. They can also be more complex, such as an intrusion detection system. All detective systems have several things in common; they look for unusual or prohibited activity. They also provide methods to record or alert system operators of potential unauthorized access. Detective controls do not prevent anything from happening; they are more of an after-the-fact measure.

Corrective Controls

Corrective counteracts something that is undesirable. Organizations put corrective access controls in place after a system experiences a threat. Corrective controls restore the system back to a state of confidentiality, integrity, and availability. They can also restore systems to normal after unauthorized activity occurs.

Recovery Controls

Recovery is a return to a normal state. Recovery access controls restore resources, functions, and capabilities after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls.

Compensative Controls

Compensate means to make up for something. Compensative access controls provide options to other controls to bolster enforcement in support of a security policy.
A compensative control can also be a substitution used in place of a control that is not possible under the circumstances. For example, an organization may not be able to have a guard dog, so instead it deploys a motion detector with a spotlight and a barking sound.

What is Data Masking?

Data masking technology secures data by replacing sensitive information with a non-sensitive version. The non-sensitive version looks and acts like the original. This means that a business process can use non-sensitive data and there is no need to change the supporting applications or data storage facilities. In the most common use case, masking limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis. Information can be dynamically masked if the system or application determines that a user request for sensitive information is risky.

Data Masking Techniques

Data masking can replace sensitive data in non-production environments to protect the underlying information.
There are several data masking techniques that can ensure that data remains meaningful but changed enough to protect it.

- Substitution replaces data with authentic looking values to apply anonymity to the data records.
- Shuffling derives a substitution set from the same column of data that a user wants to mask. This technique works well for financial information in a test database, for example.
- Nulling out applies a null value to a particular field, which completely prevents visibility of the data.

What is Steganography?

Steganography conceals data (the message) in another file such as a graphic, audio, or other text file. The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture actually contained a secret message by viewing the file either electronically or in hardcopy.
There are several components involved in hiding data. First, there is the embedded data, which is the secret message. The cover-text (or cover-image or cover-audio) hides the embedded data producing the stego-text (or stego-image or stego-audio). A stego-key controls the hiding process.

Steganography Techniques

The approach used to embed data in a cover-image is using Least Significant Bits (LSB). This method uses bits of each pixel in the image. A pixel is the basic unit of programmable color in a computer image. The specific color of a pixel is a blend of three colors—red, green, and blue (RGB). Three bytes of data specify a pixel's color (one byte for each color). Eight bits make up a byte. A 24-bit color system uses all three bytes. LSB uses a bit of each of the red, green, and blue color components. Each pixel can store 3 bits.
The figure shows three pixels of a 24-bit color image. One of the letters in the secret message is the letter T, and inserting the character T changes only two bits of the color. The human eye cannot recognize the changes made to the least significant bits. The result is a hidden character.
On average, not more than half of the bits in an image will need to change to hide a secret message effectively.

Social Steganography

Social steganography hides information in plain sight by creating a message that can be read a certain way

by some to get the message. Others who view it in a normal way will not see the message. Teens on social media use this tactic to communicate with their closest friends while keeping others, like their parents, unaware of what the message actually means. For example, the phrase “going to the movies” might mean “going to the beach”.
Individuals in countries that censor media also use social steganography to get their messages out by misspelling words on purpose or making obscure references. In effect, they communicate to different audiences simultaneously.

Detection

Steganalysis is the discovery that hidden information exists. The goal of steganalysis is to discover the hidden information.
Patterns in the stego-image create suspicion. For example, a disk may have unused areas that hide information. Disk analysis utilities can report on hidden information in unused clusters of storage devices. Filters can capture data packets that contain hidden information in packet headers. Both of these methods are using steganography signatures.
By comparing an original image with the stego-image, an analyst may pick up repetitive patterns visually.

Obfuscation

Data obfuscation is the use and practice of data masking and steganography techniques in the cybersecurity and cyber intelligence profession. Obfuscation is the art of making the message confusing, ambiguous, or harder to understand. A system may purposely scramble messages to prevent unauthorized access to sensitive information.