4.1 Basic Security Concepts

4.1.1 – Security Strategies

Most companies want to believe their computer networks are safe. They create user accounts, follow strict rules, and check for security issues. But sometimes, people try to break into these networks from both inside and outside the company. These attempts might be harmful, or just someone with computer skills wanting to see if they can get in. Because keeping information safe is so important, working in this part of technology requires a lot of focus, discipline, and a clear understanding of security concepts.

A cybersecurity framework guides the selection and configuration of devices and behaviors that keep a computer system secure. Frameworks are important because they stop an organization from building its security program in a vacuum, or from building the program on a foundation that fails to account for important security concepts.

Here are two commonly used strategies that many organizations use to guide their work in security.

The CIA Triad

The field of information security uses the CIA Triad as its primary principles of security control and management. For information and systems to be considered secure, they must have all three of these properties:

- **Confidentiality**: The information can only be read by people who have been explicitly authorized to access it.
- **Integrity**: The information is stored and transferred as intended and that any modification is authorized.
- **Availability**: The information is readily available and accessible to those authorized to view or modify it.

Note: The triad can also be referred to as "AIC" to avoid confusion with the Central Intelligence Agency.

Nearly all organizations have information which should be kept confidential. For example, the president of a public company might receive the company's financial documents from the accountant, but they will not be publicly released for weeks. Other employees do not need to see the numbers before the release date. Keeping these numbers a secret from the other employees is an example of information confidentiality.

When the company accountant transmits the balance sheet to the company president, the numbers should not change in any way. They should be exactly the same numbers when they leave the accountant and when they arrive in the president's files. This is an example of information integrity.

If the president of the company needs to review the financials right away, she can easily and reliably access those documents. There's no barrier to her being able to open or to read those files. This is an example of information availability.

Some security models and researchers identify other properties of secure systems. The most important of these is **non-repudiation**. Non-repudiation means that a person cannot deny doing something, such as creating, modifying, or sending a resource. For example, a legal document, such as a person's will, must usually be witnessed when it is signed. If there is a dispute about whether the document was correctly completed, the witness can provide evidence that it was.

The NIST Cybersecurity Framework

When we talk about keeping information safe, **cybersecurity** means making sure the computers and programs we use are secure. Information security and cybersecurity tasks can be grouped into five basic functions, following the framework developed by the **National Institute of Standards and Technology (NIST)**:

- **Identify:** Develop security policies and capabilities. Evaluate risks, threats, and weak spots in the system and recommend security controls to reduce the risks.
- **Protect:** Develop, install, operate, and retire IT hardware and software assets. Focus on security as a requirement of every stage of this operation's lifecycle.
- **Detect:** Perform ongoing, proactive monitoring to be sure that controls are effective and capable of protecting against new types of threats.
- **Respond:** Identify, analyze, contain, and eliminate threats to systems and data security.
- **Recover:** Restore systems and data if other controls are unable to prevent attacks.

Where the CIA Triad is a collection of ideas about security, the NIST framework is something that companies can apply more actively to the work their employees do. Some companies choose to organize their cybersecurity departments around these five functions. They might have job roles that are only associated with the Protect function, for example. Other job roles focus specifically on the Recovery aspect of cybersecurity.

4.1.2 – Device Security

The most basic part of cybersecurity is controlling physical access to computers and network devices. If a **threat actor** gets physical access to a computer without permission, they can do a lot of harm to the entire system. Physically touching the computer means someone can begin to guess passwords or steal a hard drive to get access to its data, among other attacks.

Computers are high-value targets for two different reasons:

- **Physical value:** Some computers are expensive because they're made with expensive parts. The computer is valuable for what it is.
- **Data value:** Almost every computer stores data of some kind. The computer is valuable for what it holds.

People who work in cybersecurity also ensure the physical security of the computers and devices they look after, as part of their job role.

Equipment Locks

Hardware locks for computers and networking equipment have been around for decades. As computers became smaller and more mobile, it became easier for threat actors to walk away with sensitive equipment. These hardware locks can attach to any device. In some cases the lock will keep the equipment in one place, and in other situations a different type of lock will prevent unauthorized people from using the device, even if they are able to steal it.

Most laptops, except ultra-thin laptops, have a small hole on the side or back. This hole is made for a special kind of lock, called a Kensington lock. This lock looks similar to a bike lock and comes with a cable. You first wrap the flexible cable around something big and sturdy, like a pole, a handrail, or other anchor point. Then insert the cable through the laptop and into the locking mechanism, locking it with a code or a key.

While it might seem like very basic security measures, many times people steal things just because they see a chance. If a laptop is left sitting alone on a table, it's easy for someone to grab it and put it in their backpack. A locking cable around a laptop makes it much harder to steal. When theft requires bolt cutters, crime goes down.

Many organizations use these locks on other devices as well. Desktop computers, monitors, and projectors are all compatible with this type of cable-based lock.

USB Locks

You can also put a USB lock on an open USB port on a computer to stop users from using these ports. The lock is easy to install and will prevent unauthorized data transfers through the USB port. It can also stop the computer from booting up from a USB drive.

Other Physical Security

In addition to locking devices directly, cybersecurity professionals also help prevent theft in other ways. This usually involves keeping servers in one room where doors are locked, and not allowing unauthorized people into areas of critical operations.

"I was working for a client who had multiple spaces in an office tower, which also occupied several other companies. The client's server room was down the hallway on the same floor. While walking past the server room one day, I noticed that the server room door was propped open with a door stop. No one was in the server room, but the door was wide open. On a floor that not only housed my client, but also several other companies. I asked them why the server room door was propped open, and they told me it was because there was no ventilation in the room, so they kept the door open to keep the servers cool. I asked if they were concerned about some random person walking into the server room. They told me "Well, no one has done it so far."

-- Greg C., security technician

All employees have a role in cybersecurity. Companies should train every person to understand how they can help support security measures, and how to confidently enforce the rules. Any person can ask

people they don't know, or people without the right security badge, to prove they should be where they are. A lot of trouble can be stopped if people using computers know about common threats and take precautions to avoid them. Many businesses make sure their workers go through training often, so everyone knows about the newest threats.

4.1.3 – Authentication Factors

Authentication is the process of ensuring that each account is only operated by its proper user. There are many different authentication technologies and methods. These different ways of authenticating a subject are referred to as **factors**.

Something You Know

This category includes anything that only the user should know. The typical example is the login credentials. Login credentials are the combination of a username and a password. The username is not typically a secret, because it's usually some combination of the user's first and last names, but the password must only be known to the account holder. Some other examples include:

- **Passphrase:** A passphrase is a longer password comprising a number of words. This has the advantages of being more secure because of its length, and easier to remember. "PurpleMonkeyDishwasher" will stay in most people's minds longer than "ox94TY8~3qio7" will.
- **PIN:** A **Personal Identification Number (PIN**) is a type of password you remember. It's also called a passcode, and it can contain both numbers and letters. Using a passcode is a fast and safe way to get into your device. Many people like to use passcodes because they're easy to remember.
- **Patterns:** Devices with touchscreens can offer the option to use a pattern lock as another security measure. This allows the user to draw a predefined pattern on a grid of 3 columns and 3 rows of dots.

Another key idea in proving who you are by using things you know is the concept of **Personally Identifiable Information (PII)**. This kind of proof is also helpful when you need to reset your account. For instance, PII is often used for security questions to check who you are when you call about your account. The person talking to you on the phone wants to make sure you are really you. For example, PII could be answers to questions like "What is your favorite movie?" "What street did you grow up on?" or "What is the name of your first-grade teacher?"

Something You Have

This category means that the account holder, or the person with permission, owns something unique that no one else has. There are several ways to authenticate a user based on something they have.

One way to prove who you are is to give each person a special hardware **token**. The most well-known one used to be the SecurID token. It creates a number code that matches a code on a server, which you need to enter to log in. The code changes about every 60 seconds. SecurID tokens were popular until smartphones become more common. Now, with authenticator apps, smartphones make it easier to use this kind of "something you have" authentication.

Something You Are

This category relies on something unique and virtually unchangeable about the user. "Something you are" authentication means using a system that recognizes unique body features. **Biometric authentication** uses special traits each person has that can prove who they are. You can use many kinds of biometric information, such as fingerprints, retina or iris patterns in a person's eye, facial recognition, or even the way someone's voice sounds to identify them.

When the system administrator creates the account, the user is there in person to have their unique body features, like fingerprints or eye patterns, scanned in to the system. These scans are saved in the security system as a template. When the user wants to log in, the system checks the biometrics that the user provides and compares them to the saved template to make sure they match.

This is a fast and easy way to figure out who someone is. If the scans match, the person is allowed in. These unique features are very difficult for someone else to copy, which makes them an excellent part of the authentication process. Another good thing is that, unlike special security devices, it's hard to lose your own biometrics!

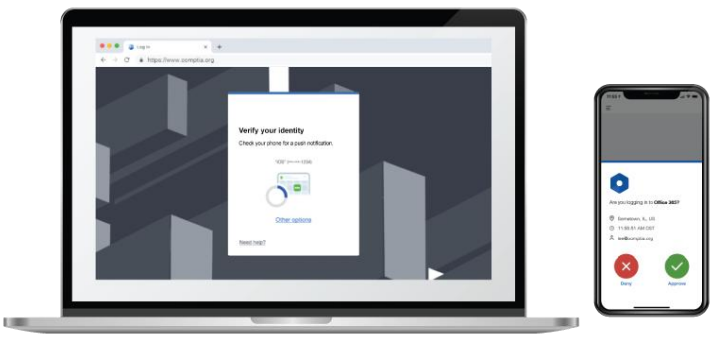
Windows 10 and 11 provide support for biometrics to authenticate you through something called Windows Hello. If your computer can use Windows Hello (if your laptop has the right camera or a fingerprint reader), you'll find this option in Account Settings. Your computer can remember your face, iris image, or fingerprint and use that to let you in. It's a nice way to get into your device without needing a password or PIN. Plus, once you're logged in, you can use your biometrics to sign in to websites or pay for things online.

The biggest issues with using biometrics are that some users find it intrusive and worry about their privacy. Also, setting up and keeping the system running can be more expensive than other authentication methods. Sometimes, biometrics can make mistakes, like not letting the right person in (false negatives) or letting the wrong person in by mistake (false positives).

Multifactor and Two-factor Authentication

Passwords alone are usually not strong enough to protect very important or high-risk applications like company networks or bank accounts. Any of the factors on this page can be a key part of **two-factor authentication (2FA)**. Two-factor authentication adds an extra step to logging in, on top of using passwords.

Some situations require even more security, as strong as an authentication system that's possible. Implementing **multi-factor** authentication **(MFA)**, using multiple authentication types, will increase the strength of the system. With two or more steps, it's much tougher for hackers to get into accounts and devices.



Single Sign-On

Single Sign-On (SSO) means that a user only has to authenticate to a system one time to gain access to all its resources. For example, with one set of log-in credentials into a Windows computer, a user will also seamlessly be logged into other Windows services, websites and programs. This makes life easier because users don't have to remember lots of different logins, which can be tiring. It's handy because you don't have to keep track of many accounts, but there's a downside too. If a hacker gets into your one account, they could get into everything else you have access to.

4.1.5 – Authorization Factors

Authorization is the process of determining what rights, or permissions, users should have on each resource, such as a file or a program. Authorization also includes enforcing those rights.

Permissions

Every organization has a huge number of programs, files, and folders in their computer system. Even smaller companies create many files in the course of regular operations. Larger organizations have the added layer of different departments with different roles, such as Marketing and Finance. Each department has specific programs and files they work with to do their jobs, and they don't need to use or look at files or resources from other departments. A network administrator will set different permissions for those files, based on who needs to use them.

Permissions can vary between systems, but the IT industry broadly categorizes permissions into different types like the ones listed here:

- **Read:** A user or group of users can view or read the file, but that is all.
- **Write:** A user or group of users can read the file, and can also modify or edit the file.
- **Execute:** A user or group of users can run a program or script from the file.
- **Delete:** A user or group of users can remove the file.

For example, a company may have a mission statement on how they will conduct their business. Employees may want to review the document from time to time, but no one should change the mission statement. This document has "read-only" permissions.

Network administrators can also set permissions at different levels. For example, the company's brand directory, or entire set of files, could have one set of permissions such as "read-only" to make sure that everyone in the company uses the same set of logos and colors. A company might also set specific permissions that apply only to a single folder or small group of files.

Network administrators can also assign permissions to individual users, or to groups of users. For example, the entire Development team may need to read or to view the schedule for project A, but only the individual project manager should be able to edit or write to that schedule. In other cases, an entire department has different levels of permission related to a directory, but members of other departments can't access that set of files at all. Financial and human resource files, containing sensitive information, fall into this category. Setting group permissions makes the IT department's job much more simple.

Least Privilege

In IT, there's a rule called **least privilege**. This rule means that a user only gets the access they need to do their job, and nothing more. You could think of it like keys to a building. Employees only get keys to the rooms they need to go into and are kept out of places they don't need. This helps to reduce the risk of security breaches, simple mistakes which expose a network, or introducing software which may corrupt system data. The concept of least privilege makes IT management quite a bit easier.

When you give more people access or permissions on a computer or network, you're taking a bigger risk that someone might use those permissions in a way they shouldn't. The user could misuse that permission intentionally, or they could cause a problem by accident. To keep things safer authorization policies make sure people only get the special access they really need, based on the concept of least privilege.

Think of it like an invite-only party. If you're not on the party's guest list, you can't come in. In the same way, access controls work by saying "no" to everyone unless there's a specific "yes" that lets them in. This is called "implicit denial." If there's no clear rule that says you can have access, then the answer is automatically no.

Administrators and Standard Users

Some special accounts can do anything they want on the entire computer system. On Windows and Apple macOS these accounts are called Administrators, and on Linux they're called the Root user. Because these accounts can change anything on the computer, network administrators must be extremely careful when assigning these special user types.

Just below the Administrator, there's a type of account called a standard user. Standard users can still do their job tasks, such as opening files and using programs, but they can't add new software or modify important system settings. The goal for the standard user permission level is to let the workers do their jobs without needing to ask the IT department for help all the time, while also keeping the computer safe.

In many organizations, it's common to assign these standard permissions to people using the computers or workstations. This helps to limit changes from being made and lowers the risk from malicious events. For a virus to get into a computer or network, it has to run, just like any other program. That's why not allowing the installation of new programs is a key step in keeping things secure.