Bellevue University

Principle of Separation

In Cryptography

Timothy Jelinek

CYBR250-T301 Intro to Cyber Threats

10/15/2023

A famous principle in today's age is separation of duty. The idea behind the separation of responsibility is to make things more secure by breaking up different pieces of a whole to other people so that not a single person has access to the whole. This can be seen in many scenarios, from payroll department donation centers to local retail stores. In the store I work at, I have an authority level. Other people can access different things within the store's computers and equipment based on their authority level. A manager will have an authority level of five where they can do any items related to the store up to managing the employees and who is on the schedule. I have an authority level of three, so I cannot see what my managers see when it comes to employees; however, I have access to doing different tasks on the computer than others at level one and the ability to price override and do returns.

Separation of duty is when not a single user should be given enough privileges to misuse a system independently. An example of this would be that a person who authorizes a paycheck should be different from the person who prepared the compensation. You can enforce the separation of duties statically by defining roles and giving them to specific people or by dynamically executing control when the person needs access. An example of using dynamic separation of duty would be using a two-person rule. Any authorized user can be in the first person in the two-person direction, while the second person would be a different authorized person than the first. This is an excellent plan of action to minimize the risk of an inside person attacking your system. Separation of Duty can be instrumental in keeping things safe in cryptography. A way to use separation of duty is by isolating sensitive systems from less sensitive ones by using a firewall. Another way is by assigning specific roles to different users based on their job responsibilities to limit access to the system. A third way to use separation of duty is by dividing the cryptographic keys into multiple parts. By dividing up the keys, you can make it harder for attackers to obtain the entire key.

After reading about separation of duty, I learned that separating powers and access among your peers at your job is essential to ensure everything is legitimate and secure. A brand-new cashier would be dangerous to have access to the schedule and payment services at the business. Separating duties also allows for integrity to remain in place by the people preparing the checks, not the same people verifying them. In computer systems, it is also essential to separate duties so that an intern cannot access all of a business's vital information and data. When encrypting data, you can also break keys up and store them in different areas, making it harder for a potential attacker to obtain an entire key. No one outside the business should touch all sizes on a business's website. Giving authority only to the people who feel specific parts of the site or system are vital to keeping information private and company records.

In my personal life, I also practice separation of duties. I am one of the only people with the password and access to my phone. At home, everyone in the household has access to the password and access to the router to make changes to keep our internet secure. We do not have access to each other's bank accounts, so critical, private information stays private. However, everyone has everyone else's phone number to keep in contact in an emergency. By applying separation of duties in your everyday life, you are keeping yourself and the people close to you safe.

Sources:

"Separation of Duty (SOD)" NIST, https://csrc.nist.gov/glossary/term/separation_of_duty.

It was accessed on 15 October 2023.