Software Security

By Christopher Lebovitz

Date: 4/19/2021

Sofware security Is a part of the Software Development Process. People and policies that

ensure a program's confidentiality, integrity, and availability. Software security is a relatively new concept to computer science. Most of the focus in the late 1990s and early 2000s was to protect the physical access to information from people who wish to access the data for malicious reasons. But things began to change when bill gates released a memo instructing the Microsoft employees to look at security from the emerging internet and physical access. Since then, the process has expanded into making sure that the programs that connect to those systems are secure to prevent hackers from gaining access to their servers.

A program is said to be secure software when the program is being developed with security in mind. Security for applications is a continuous battle between security specialists who identify threats and attacks and hackers trying to access a program or application to get to the data stored on the servers. To create applications that are software secure the following activities should be completed these include: developing the concept of the application, gathering functional requirements, defining the control specifications, for example, creating an access control list for admin on programs or defining role to restrict the user to certain parts of an application, design review, peer reviews and demoing the app to the product owners, software testing, change management, and supporting the app after it has been launched.

There are several things a product owner needs to keep in mind so that the software is developed securely. Protection from disclosure means when to disclose that there are vulnerabilities to the software to not alarm people and protect public image. Protection from alteration so that no one outside the application or network can alter it to access sensitive data. Protection from destruction prevents most people from deleting data from the program; most companies have that ability only reserved for system admins. The product owner needs to understand the type of people who will be using the app and why they are using it to know where potential vulnerabilities may be found. They also need to understand who needs to see what, for example, if it was a timekeeping system does an employee need to see everyone's timesheet or be limited to them only as well? Do they need the ability to approve their own timesheets?

Another thing to keep in mind is there any need to audit things, if so, there needs to be a place to store information that happens on the system to build some sort of historical information. And lastly, the product owner needs to understand how the management of the application is handled, how long someone can be in the program with no activity, and how to handle incorrect inputs. As long as this is kept in mind when the program is being developed, what will result will be secure software at the end of it.

There are several tools available that will ensure that an application is secure. There are

dynamic application security testing tools to communicate with an application throughout the website to identify security vulnerabilities. The type of testing it does is black-box testing. It works without knowing how things are working internally. It is solely focused on input and output, and they have no access to the program's source code. This tool is perfect for a company that wishes to build a web application such as a store handling transactions and shipping formation. The good thing about DAST tools is that I simulate a malicious user and giving a real sense of how an actual attack can occur. They also scan year-round, constantly searching for vulnerabilities with allows companies to find exploits that were introduced before they become a real problem. The downside of these tools is that they cannot cover every possible type of attack, so the attacks the tool can emulate are limited. Also, some tools do not work well with applications that use javascript and flash.

Data loss prevention software protects data and prevents them by monitoring the data. There are three different way that the software scans the data when an employee access the information and is working on it, when the data is moving through the network, or when the data is sitting on the database. There are also three different ways that this tool can be deployed in the system. Standard security measures use firewalls to prevent access to the network, intrusion detection systems to warn the network administrators, and antivirus software that scans the network and connected system to check if any trojan horses or any other virus have been installed while being attacked. Advance measures use machine learning to detect things that are out of the normal. Some examples of what these measures can see if data is being accessed at irregular hours, odd email exchanges, or by monitoring user activity for uncommon data access. The last way the tool can be implemented is as a designated system that prevents those who are authorized to view sensitive data from copying it, intentionally or not. The system uses several different ways to classify information as sensitive. Access control list can be implemented which say who can view what, data matching, and data fingerprints.

Intrusion detection systems are a significant tool that is deployed on the network to protect it. It monitors a network or system for malicious activity or violation of policies. There are two types of intrusion detection systems network-based and host-based. Network-based

intrusion detection systems monitor the network traffic that comes into the network. Host-based is when the system monitors critical applications or files. As a whole, intrusion detection systems do not prevent access to the network. To both monitor and control intrusions, one would need an intrusion detection and prevention system. to prevent access, it uses several different ways it can prevent access, I can change the settings of a firewall to make it harder for the attacker to gain access or trap the hacker in a honeypot and trap them there to gain information on how the attacker gained access to the network.

To ensure that I securely develop software, there are several practices I will follow. The first one testing input is the most obvious one, but every approach must be considered. Attackers can attempt to enter junk data to perform a buffer overflow and make your system go offline, or they can make SQL attacks if fields are connected to the database. I can also make sure I only store the files and documentation that I'm currently working on. I would do this just if my system is compromised, and I can limit the information the attacker can have access to. Also, I will only use trusted libraries for whatever programing language I will use at my job. This will limit the possibility of back doors existing since the libraries will only be from trusted sites.

Limiting privileges is also something I can do when working on projects. However, who gets what permissions is more of a thing provided to me by the product owner. Doing so will decrease the possibility of error from people who do not work the process. Peer review is another critical aspect. The more developers who can see your code and critic, the more they can identify potential risks and concerns that your code could possibly introduce. Outsiders can also be brought in to look at how the software development cycle is being run. I will keep up with emerging technologies and see if there are any new exploits have been discovered by security professionals. Following these practices will ensure that I create secure applications for any job I choose to do.

Looking at the things discussed in this paper, we have learned how important it is to have a secure program and how we developed programs with security in mind. We talked about how an attacker can gain access and how, if following appropriate practices, we can mitigate or prevent them from gaining access to the internal network and systems. We also looked at a couple of tools to monitor the network and connected system and avoid access to those said things. Security is a paramount concern in every aspect of a business, from informing people of spam emails and phishing attacks to securing network traffic using an intrusion detection system.

References

Data loss prevention software. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Data_loss_prevention_software

Software development security. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Software_development_security

The Past, Present and Future of Software Security. (n.d.). Retrieved from https://threatpost.com/past-present-and-future-software-security-091311/75644/