Binaya Rimal

04/24/2025

Module 8: Journal

In this course, we learned about various ways to protect assets against cyber threats. We explored in depth the use of secure coding standards and best practices. Adhering to secure coding practices reduces risks by addressing common vulnerabilities such as buffer overflows, SQL injections, and improper error handling. Key practices include enforcing strict data types, validating and sanitizing user inputs, and implementing exception handling. These measures help prevent unauthorized access, data breaches, and application crashes.

Secure coding practices, such as the principle of least privilege, ensure that the minimum level of access is granted only after proper authorization and verification. This works in conjunction with the Default Deny coding standard, which denies access by default and only grants it once the user has been properly authenticated and authorized. Developers should protect memory by ensuring that memory allocation is based on the size of the object type, preventing buffer overflows. Additionally, developers should ensure that operations on signed integers do not result in overflow, as this could lead to unpredictable behavior and vulnerabilities in the system. These are a few of the best practices among others that are essential for securing a system.

Security should be incorporated at every step of the development process and should never be treated as an afterthought. By embedding security practices early in the design, coding, and testing phases, developers can proactively identify and address potential vulnerabilities before they become major risks.

A big reason why security should be a top priority is that the cost of dealing with security breaches can be significant. The immediate expense of removing the threat often involves extensive manpower which can be costly. Beyond the technical response, companies may suffer direct losses from stolen assets, including financial resources or confidential customer data. When customer information is compromised, businesses risk lawsuits and the loss of public trust. Perhaps most damaging of all is the long-term impact on a company’s reputation, which can lead to reduced customer loyalty, and decreased market value.

Another essential practice for safeguarding digital assets is adopting a Zero Trust security model. Before companies assumed everything inside an organization’s network is safe, Zero Trust assumes that threats can originate from both outside and within. Given today’s landscape, where employees work remotely and data flows in and out of cloud services, it's critical to authenticate and validate every user, device, and access request, regardless of location.

For most companies, we recommend a combination of modern security strategies, including automation, encryption, the "Triple A" model (Authentication, Authorization, and Accounting), and Defense in Depth, which layers multiple defenses to slow and deter attackers. As threats evolve, organizations can also benefit from integrating artificial intelligence and machine learning into their security infrastructure to detect anomalies, predict vulnerabilities, and respond to incidents in real time.