Portfolio Reflection

“Security” and “Data Privacy” have become buzzwords topping headlines over the last several years. Technology has grown at a rapid pace; roughly a decade ago, the first real “smartphone” was released to the public, whereas today most homes have “smart” appliances, digital assistants, and all kinds of data-consuming applications they use on a daily basis. In a world driven by technology, it is important now more than ever that developers and tech companies work towards the most secure version of their product as possible.

Security-focused development starts at the beginning of the development cycle, and persists throughout each and every aspect of the design and functionality. This includes security-focused architecture to systems, adoption of secure coding standards, and integrating security features as early as possible. Security standards and policies vary depending on the organization, but are an essential foundation for building secure systems and securing both company assets and user data. “One of the primary purposes of a security policy is to provide protection - protection for your organization and for its employees. Security policies protect your organization’s critical information/intellectual property by clearly outlining employee responsibilities with regard to what information needs to be safeguarded and why.” (Dunham, 2020).

Another important aspect of security-focused development is the evaluation of risks and benefits to your system. Risk assessment tools and frameworks, like OWASP, help developers locate potential vulnerabilities in large code bases, including those relying on external dependencies. Reviewing the code base, either manually or with automated tools and static testing frameworks is a major step towards ensuring the security of a system or application. “A secure code review is a specialized task involving manual and/or automated review of an application’s source code in an attempt to identify security-related weaknesses in the code. … The goal is to arm the developers with information to help them make the application’s source code more sound and secure.” (Mitre Corporation, n.d.).

There are several different models for implementing security policies across a system or network of systems. These change and evolve over time, as the needs of users and organizations change with the shifting technology. The end goal is always the same: how to give the best user experience to users while providing the most security to systems and sensitive data. One such model is known as the Zero-Trust model. This model focuses around point-to-point authentication, most typically through a service such as SSO (single sign-on), which verifies the users information and places policies on their permissions and system access based on predefined policies. This model also helps prevent unwanted travel throughout the system by modularizing the way users access different parts of the system, as well as requiring authentication at each step. “‘Zero trust’ is a phrase first coined by John Kindervag of Forrester in 2010 to describe the need to move security leaders away from a failed perimeter-centric approach and guide them to a model that relies on continuous verification of trust across every device, user and application. It does this by pivoting from a ‘trust but verify’ to ‘never trust/always verify’ approach.” (Kueh, 2020). It is important as developers to implement these security policies and best coding practices in place at the very beginning of the development life cycle. Of course, it helps protect the systems, data, and company from an ever increasing risk of digital attacks, but it also mitigates the need for lengthy, and often costly, troubleshooting, patching, and general security maintenance after product release, as hopefully most if not all security vulnerabilities are addressed during the development process.

**Bibliography**

Dunham, R. (2020, May 5). *Information Security Policies: Why They Are Important To Your Organization*. Linford & Co, LLP. https://linfordco.com/blog/information-security-policies/

Kueh, T. (2020, January 15). *A Practical Guide to Zero-Trust Security*. threatpost. https://threatpost.com/practical-guide-zero-trust-security/151912/

Mitre Corporation. (n.d.). *Systems Engineering Guide: Secure Code Review*. Mitre. https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/secure-code-review