Jack Muterspaugh

11-16-2024

Categorizing data as “at rest”, “in motion”, and “in use” can help us to understand and visualize data at different points in its lifecycle. Data “at rest” typically refers to inactive data that is being stored on a database, hard drive, etc. Data “in motion” means data that is being transferred from one location to another. Data “in use” is data that is actively being used or processed by an application. Categorizing data like this can help to mitigate security risks associated with the different states that data can be in.

When data is transmitted in cleartext, it is not encrypted, which can lead to a lot of security risks. Some common attacks associated with this are packet sniffing, and man-in-the-middle attacks. During these attacks, an attacker can monitor or modify data as it travels across a network. *MITRE* points out that unencrypted data transmission allows attackers to gather sensitive information like personal data and credentials. This flaw can be both software and network related. If the software has inadequate encryption in place then it introduces vulnerabilities. If the network has insecure transmission methods then this can cause issues as well.

Tools such as Wireshark can be very useful when it comes to identifying where a security flaw might take place. Wireshark captures network traffic in real-time and can be used to identify clear text data transmission and exactly where it's taking place. This can assist in identifying patterns that could be an indication of malicious activity or potential security flaws.

To prevent data at rest exploits, it is important to implement a secure encryption method such as Bcrypt, to ensure that the data is unreadable to an unauthorized user. It is also important

to perform regular security audits, and system updates within the database to ensure that there are no vulnerabilities that could be exploited by a malicious actor.

Encrypting data is a crucial technology in this area, Bcrypt in particular is a great technology to use for doing so. Bcrypt is an advanced tool for securing data at rest, more specifically hashing sensitive data such as passwords. Bcrypt employs a salting technique and hashing to make brute-force attacks virtually impossible. The Bcrypt algorithm is designed to be very slow, so if an attacker were to gain access to the encrypted data, it would take extensive periods of time to decrypt the data. When it comes to securing data, Bcrypt is a great option to ensure that encrypted data remains secure. Overall, encrypting data is crucial in maintaining a secure system to ensure there are as little vulnerabilities as possible.