Joe Workman

Developing Secure Software

Operations with Degraded Security

After security has been compromised, how can a system function and what actions need to be controlled? These questions can be answered using the ResiliNet model. Using redundancy, a system can be built to be resistant to failure. When a part of the system fails, the system enters a degraded state and can still operate at this level until the part of the system that has failed can be restored. Many have attempted to apply this theory to security but have ultimately failed showing that the system is only as strong as its weakest part when it comes to security.

Typically when a hard drive fails in a RAID configuration, the system takes a performance hit until the drive can be replaced. However, the system can still be used. With a security breach, the damage is usually so invasive and widespread throughout the system that the solution is to wipe the entire system and re-install.

Using the ResliNet model, a system should defend against attacks, detect intrusion, remediate an attack to stop it from spreading, and recover after after data has been compromised restoring the system to a previous state. Many companies use an approach to detect a security issue, shut down the system, repair the system, and then bring the system back online. The problem with this approach is that it does not allow any data to be collected about what caused the security issue and if any data was compromised. The better approach is to have the system move into a remediated state while still operating to allow information to be collected about the threat and learn how to prevent it in the future.

There are a few different approaches that are discussed in this article. The first is ignorance. Operating the system without knowing of an infection. The second is to respond to

an attack and recover without learning anything about the threat and what caused it. The third approach is to isolate the threat and the treat it after learning about what caused it. The fourth approach is to silently monitor an attack to try and learn where the breach came from. This can be useful if a system should not reveal that it has been compromised to other systems or the public. The final approach is to just live with it and keep using an infected system normally without trying to fix the problem.

These different approaches need to be evaluated based on the sensitivity of the data being protected and the risks of that approach. While it may not seem like it, there may be times where allowing a compromised system to keep running in order to collect data about the threat is the desired action in order to increase future security or warn other people about the threat and how to stop it.

Simson L. Garfinke George Dinol, *Operations with Degraded Security*, www.computer.org/plugins/dl/pdf/mags/sp/2011/06/msp2011060043.pdf