What is Fault Injection Attack (FIA)? Is it worrisome?

Fault injection is the deliberate act of creating errors in a system. The goal of this is to analyze how the system behaves under pressure.

Vessels are machines with many parts that work to ensure safe, successful voyages. Software is similar. Like software development, shipbuilding involves a number of precise steps and techniques. Then, once everything was done, the crafters tested their creation in different conditions to make sure the ship was safe and operating as designed. Nearly all of the best software we use today go through tests to make sure they're safe.

One of such tests is fault injection. Compared to shipbuilding, this method is like marine engineers deliberately punching holes in their ships to see how to handle when the ship sinks.

What is Fault Injection and why is it important?

Fault injection is the deliberate act of creating errors in a system. The goal of this is to analyze how the system behaves under pressure. Hardware and software engineers often cause errors in their hardware or software for a number of reasons.

First, they wanted to detect and resolve errors that could arise outside of the lab's controlled environment. This is important because they have no control over the conditions under which customers will use their products. Heat can affect the components or materials that hold the components together; server failure can cause entire regions to lose access to favorite streaming services; attackers can cause bugs that break security features. When such events occur, developers and device manufacturers want to ensure their products still protect data integrity and user safety, or adjust load allocation to minimize service interruption.

Ultimately, Fault injection is necessary to make the application and hardware safe, secure, and reliable. Likewise, Fault injection helps manufacturers protect intellectual property, reduce the risk of loss, and preserve customer trust. You wouldn't deposit your money in a bank if their app kept crashing would you?

How does Fault Injection Attack (FIA) work?

Manufacturers intentionally perform Fault injection to detect bugs that can affect product security. There is nothing to prevent attackers from doing the same to expose weaknesses in the system and exploit them. After all, the tools used to perform Fault injection are public and the methods are not overly complicated.

Furthermore, experienced attackers can get creative with their own methods and push the system beyond the norm. At this point, you need to know that Fault injection can be physical (in hardware) or digital (in software). Likewise, the tools and methods used in Fault injection attacks can take both forms. Manufacturers and hackers often combine physical and digital tools in their testing and attack processes.

Some of the tools used to perform Fault injection are FERRARI (Fault and ERRor Automatic Real-time Injector), FTAPE (Fault Tolerance And Performance Evaluator), Xception, Gremlin, Holodeck and ExhaustiF. Meanwhile, FIA methods typically involve bombarding the system with intense electromagnetic pulses, which increase the ambient temperature, lower the voltage of the GPU or CPU, or cause a short circuit. Using FIA tools and methods, they can damage systems long enough to take advantage of resets, bypass protocols, or steal sensitive data.

Prevent FIA attacks

You don't have to worry about preventing FIA attacks if you're a regular consumer. That responsibility rests with the equipment manufacturer or software developer, just as the safety of the ship is the job of the crew. Manufacturers and developers do this by designing security protocols that are more flexible and make data extraction difficult for hackers.

However, no system is perfect. Attackers are constantly developing new attack methods, and they are not limited in how to apply those methods because they don't play by the rules. For example, hackers can combine FIA ?? with a Side-Channel Attack (SCA), especially if their access to the device is restricted. The development team must acknowledge this fact in designing resilient systems and planning their Fault injection tests.

Should you worry about the FIA?

The FIA ??does not directly affect you. It is more likely that cybersecurity threats affect you personally than Fault injection attacks. Besides, the FIA ??is rarely secretive. An attacker would need physical access to your device to perform the attack. In addition, Fault injection methods are generally invasive and result in some degree of temporary or permanent damage to the system. So you will most likely notice something is wrong or

be left with a device that you cannot use.

It's worth noting, of course, that an attacker could have stolen sensitive data by the time you notice the tampering. It is the responsibility of the manufacturer or developer to prevent an attack in the first place and improve the security of their product.

You finished reading the article "**What is Fault Injection Attack (FIA)? Is it worrisome?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com