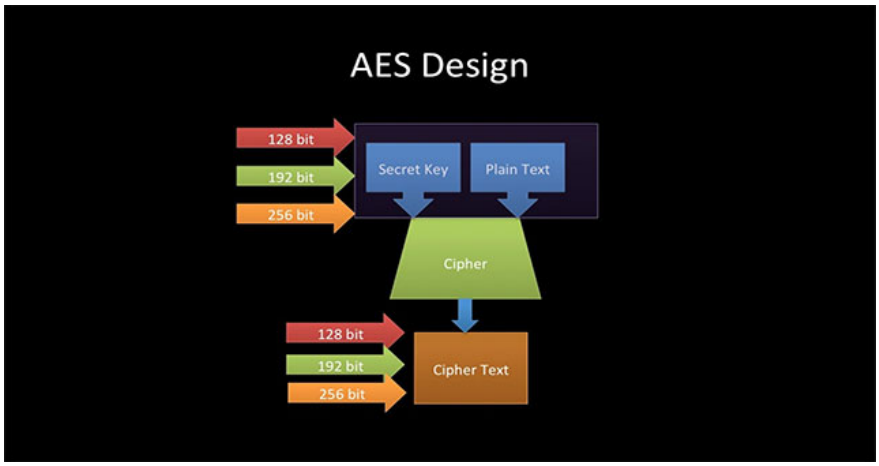
Application protection against DFA attacks

Differential Fault Analysis, also known as DFA, is an attack technique designed to recover cryptographic keys from the application ...

2001 marked an exciting time for cryptography in particular and information security in general, when Advanced Encryption Standard (AES) - a block encryption algorithm The new has been completed, while helping the high-performance secure encryption algorithm become more popular and accessible.

Designed to replace older cryptographic algorithms that have begun to show weaknesses in mathematics and at the same time vulnerable to increasingly powerful computing power in the hands of attackers, it is possible said AES has become a tool to regain power for users who are trying to protect their data against growing threats. Of course, hackers quickly realized that the Brute Force attacks in general and attacking the mathematical characteristics of AES in particular were no longer as effective as before, and instead needed an approach. new.



1. Scary data breaches in China: Information about the 'fertility' of more than 1.8 million women leaked

And just a year later, the hacker had a worthy response to AES. Differential Fault Analysis, also known as DFA, is an attack technique designed to recover cryptographic keys from the application by injecting a password 'error' into the application when running, and observe changes in the behavior of the application. Errors can be injected in different ways, such as different energy levels in hardware devices or changing the memory bit in the software.

For example, a smart card containing an embedded processor may be subjected to high temperatures, unsupported or overclocked voltages, strong electric or magnetic fields or even ionizing radiation and affect activity. processor dynamics. The processor may start exporting incorrect results due to physical data corruption, which can help cryptographic analysts infer the instructions that the processor is running or its internal data state what.

Attackers inject errors at various parts of the application, until they find a place where the output data change error appears in a specific way. DFA and some operations can allow cryptographic keys to be recovered. When those keys are restored, all data encrypted with them is vulnerable and at risk of being compromised.

1. There were 12,449 serious data breaches recorded in 2018, an increase of 424% compared to 2017

Originally, DFA was a major attack against hardware devices, where machine code was often not available for attackers to access. But in the case of software, things are much simpler, because often the cryptographic keys are clearly displayed inside the application code, so tools like the separator can easily be displayed. information about them. For a long time, if a piece of code is being used to perform encrypted logging, it will be kept in a secure environment, where attackers cannot easily access the application code to find those keys.

However, this has changed dramatically, as consumers today have a lot of applications on mobile phones, desktops, smart TVs and even cars. Software applications need to be protected for their program segments and cryptographic keys. Whitebox encryption was introduced in 2002 to address concerns about this issue, ie the same year the first article about DFA was published.

Specifically, Whitebox encryption has been introduced in order to provide secure encryption deployment methods in applications where an attacker can manipulate code and data at will. It is understandable that Whitebox encryption is a way to have the same output for a given input as a conventional crypto deployment plan, but the way it is implemented is completely different from cryptographic deployment. standard. This makes it difficult for an attacker to grasp what's going on.

1. McAfee expert explained how deepfake and AI are drilling through the cyber security wall

Because of the difficulties encountered when dealing with Whitebox encryption on hardware devices, attackers decided to start using DFA as a technique against whitebox encryption in software deployment.

DFA is becoming more and more popular. Security researchers are talking more about DFA attacks at conferences, forums, and they conduct DFA attacks on both hardware and software and then explain each step. DFA is no longer a limited range attack in high-end security academies or institutes. Real-world DFA attacks are taking place more and more, and with the popularity and 'weaponization' of attack codes, the frequency of reported DFA attacks will increase even further. Future.

As DFA advances in efficiency and popularity, you must ensure that your defense measures can keep up and meet the security requirements of the segments. In-app coding program. Of course, there are a number of steps you can take to ensure that your system is sufficiently resistant to DFA attacks.

1. Supercomputers can completely detect cyber threats

The first is to ensure that you are using a modern whitebox encryption implementation method, designed to protect against DFA, as well as being tested against the latest versions of the form. this attack. Because attacks often develop sophisticated over time. It's important that you use whitebox implementations that are modern enough to keep up with attacks that are sophisticated and rapidly growing day by day.

Secondly, you should ensure that your application is protected by the app shielding to make the attacker more complicated to execute DFA from the beginning. Applications that are set up with obfuscation will make it more difficult for an attacker to determine what is the right location to inject the error, and the application can also detect when attacked, and Immediately act to stop the attack before they progress to a more dangerous stage.