Silencing Hardware Backdoors

By: Conrad Buerger

For: Walter Schilling

Developing Secure Software

SE-4930

February 5th, 2012

The article “Silencing Hardware Backdoors” talks about how there can be ways to maliciously use hardware to break into systems. The first major topic that the paper brings up is how there are multiple ways to use the hardware to maliciously attack a system. Another major topic in this article talks about the different triggers that can create backdoors in hardware implementations.

The article brings up three major ways that hardware can be used to prevent malicious attacks against a system. The first one is power resets which limit the system from detecting how long it has been active if the malicious part of the hardware is built to go active after a certain amount of time. The second method that the article talks about is called data obfuscation, which “encrypts input values to untrusted units to prevent them from receiving special codes, this preventing them from recognizing data-based triggers.” (2) The third and final method that is talked about in this article that can prevent malicious hardware from activating is called sequence breaking. This method “pseudo-randomly scrambles the order of events entering untrusted units to prevent them from recognizing sequences of event s that can serve as data-based triggers.” (2) These three types of ways to prevent most hardware systems from doing malicious tasks. With that said, the article uses the OpenSPARC T2 multicore chip to show how these methods work.

The authors of the article continue on to describe the two main triggers that are coupled with interface devices. The first of these three triggers is called a ticking time bomb. Essentially how a ticking time bomb works is to set a backdoor to trigger after a set amount of time goes by. An example that they give that relates to the OpenSPARC T2 multicore chip is that a backdoor could be opened after a certain amount of clock cycles has gone by. This type of trigger is hard to catch in validation tests because no one knows how long one has to wait in order for the time bomb to go off and validation testing only lasts for a certain period of time that may not be enough to encounter the time bomb.

The second of the three triggers is called a cheat code. A backdoor can be created by a special sequence of input characters. There are two ways that a cheat code could be entered into a system. The first method being that the cheat code could be entered in at one time, thus giving this type of cheat code entry the name single-shot cheat code. The other is called a sequence cheat code which involves the cheat code being entered in multiple inputs. This involves the cheat code being entered in smaller chunks over a period of time. Either of these methods can be applied to the OpenSPARC T2 multicore chip to open a backdoor if the chip has a cheat code backdoor implemented within the hardware.

In conclusion, this article brings to light the ways that hardware can be maliciously used to gain access to the system that contains sensitive information. In this article we also learned how we can trigger hardware systems to open backdoors. Overall, we can see that not just software has security issues, hardware does as well.