ECEN 426: Security of Embedded Systems **Fall 2021**

Lecture 6: Hardware Trojans

Lecturer: Jeyavijayan Rajendran *Scribe: Michelle Kim*

Note: *LaTeX template courtesy of UC Berkeley EECS dept.*

6.1 Trojan insertion taxonomy

The trojan insertion taxonomy consists of the design phase, abstraction level, activation, effects, and location, shown in Figure 6.1. The trojan taxonomy is explained further in the reference [1]. Lecture 6 focuses on the abstraction level, activation, effects, and location. The hardware abstraction level consists of the system, RT, gate, transistor, and physical level. Figure 6.2 shows the details of the hardware abstraction level. Software tools are used at all stages. Activation is either always on or triggered. The triggered type of activation can either be triggered internally or externally. There are time based and physical condition internal triggers. External triggers can be caused by the user or the component. Some of the different types of effects are change function, change specifications, leak information, or denial of service. Location can be in the processor, memory, I/O, power supply, and clock.

6.2 Trojan examples

1. Leak encryption key

   Leak encryption key, displayed in Figure 6.3, is an input triggered trojans which are triggered by rare events and physical access is required for the attackers. The phase is design, abstraction is at the RT level, activation is user input, effect is leak information, and location is the processor and I/O.

2. Denial-of-service under special input

   In Figure 6.4, the denial-of-service under special input is triggered by an undefined key on the keyboard. 9.4% less flip-flops are used and margins are created to hide trojans. The phase is design, abstraction is RT level, activation is user input, effect is denial of service, and location is the processor and I/O.

3. Faked output

   The faked output trojan is shown in Figure 6.5, and the phase is design, abstraction is RT level, activation is user input, effect is modify, and location is the processor and I/O.

4. Buffer overflow

   Buffer overflow is an example of targeting design flaws, shown in Figure 6.6. Many design specifications do not consider potential trojans. Phase is design, abstraction is RT level, activation is user input, effect is leak information, and location is processor's I/O.

5. Attacking the Transmission Protocol

   There is communication between the desktop computer and FPGA. In this example, the unaffected output can be read at 9600 baud rate. Baud rate is the rate at which bits are transferred in a communication channel. In Figure 6.7, if you increase the sampling frequency to 19200 baud rate at the receiving end, the information from the trojan which is sent at certain intervals can be read. This trojan is always activated, leaks information, and is located at the processor's I/O.

6. Time Bomb

   There is a very large counter such that it bypasses any functional tests. The trojan is triggered at a large time value of N where the system while the system is still operational in the field. In Figure 6.8, the time bomb trojan can be combined with any other payload. The phase of this trojan is design and the abstraction is the RT level. The activation is time triggered and effects are a change in function. This trojan is located at the processor's I/O.

7. Controlling the device

   This trojan plays with the protocol. This trojan has multiple effects like denial of service or leak information. The phase is design and abstraction is the RT level. Activation is user input and its location is the processor's I/O.

8. Stealing data from keyboard

   This trojan leverages peripheral devices as the path of attack. The class example, highlighted in Figure 6.9, shows that pressing the 'Caps Lock' button, the entire key is acquired.

6.3 Figures

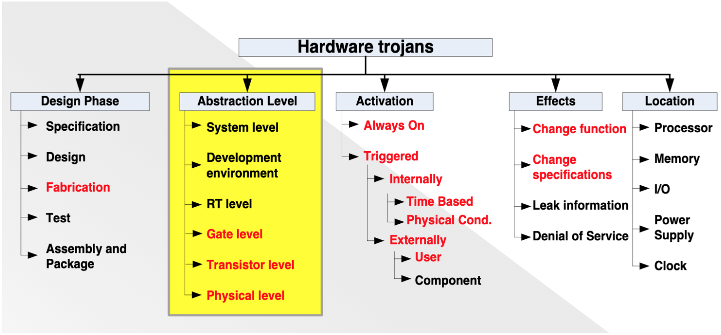


Figure 6.1: Trojan insertion taxonomy

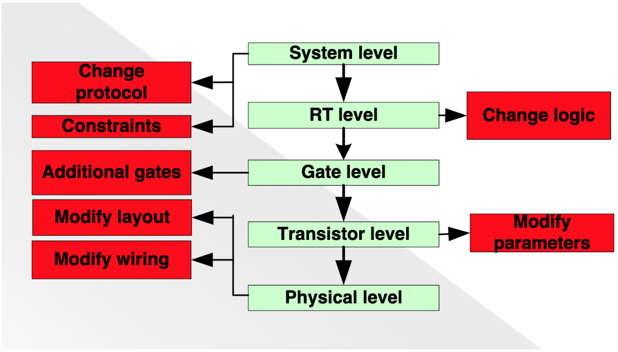


Figure 6.2: Hardware abstraction level

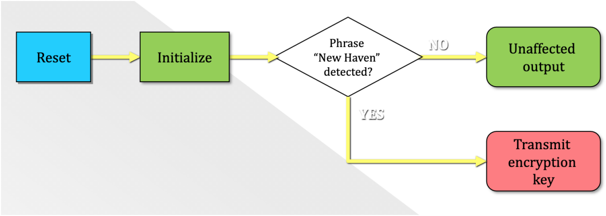


Figure 6.3: Leak encryption key

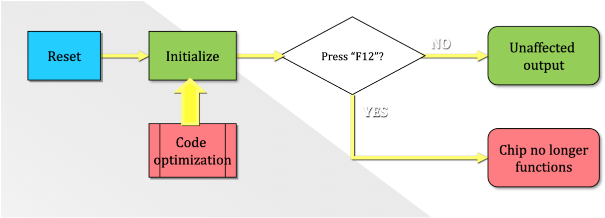


Figure 6.4: Denial-of-service under special input

References

[1] Ramesh Karri, Jeyavijayan Rajendran, and Kurt Rosenfeld. Trojan taxonomy. In *Introduction to hardware security and trust*, pages 325–338. Springer, 2012.

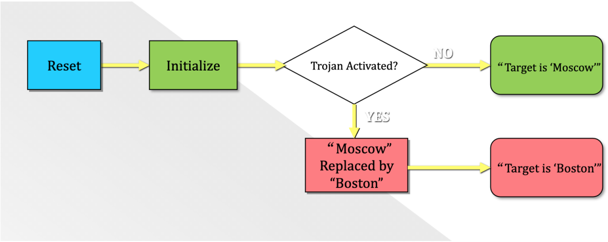
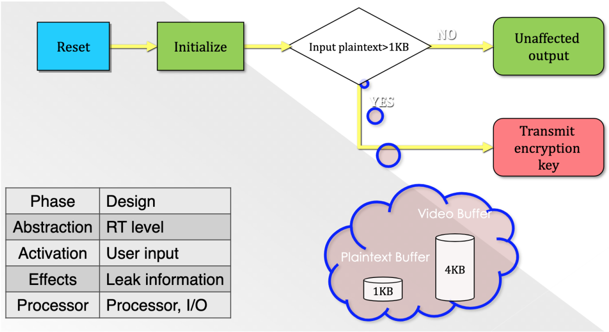


Figure 6.5: Faked output



Phase	Design
Abstraction	RT level
Activation	User input
Effects	Leak information
Processor	Processor, I/O

Figure 6.6: Buffer overflow

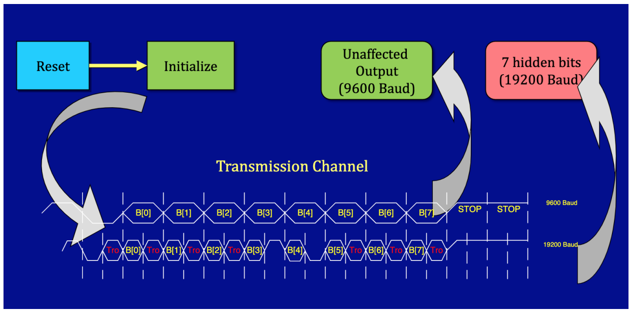


Figure 6.7: Attacking the Transmission Protocol

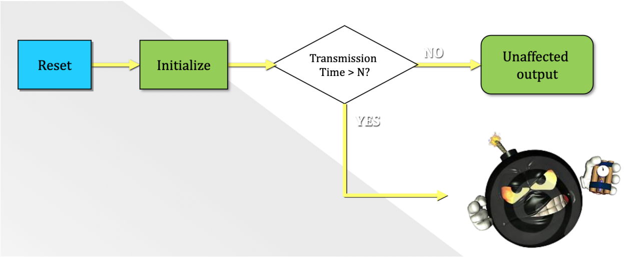


Figure 6.8: Time Bomb

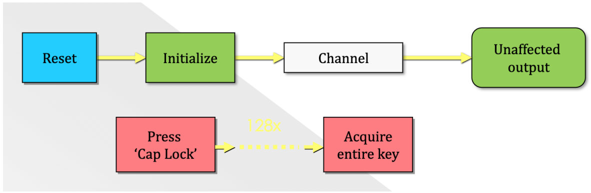


Figure 6.9: Stealing data from keyboard