Verification and Detection of a Wireless-Leakage Hardware Trojan Horse with Covert Channels

Yancang Chen¹*, Ying Zhou¹, Pei Wei¹, Sai Sui¹, Yaxin Zhao¹, Minlei Zhang¹ and Lunguo Xie²
¹Luoyang Electronic Equipment Test Center, Luoyang, China
²National University of Defense Technology, Changsha, China
*Corresponding author

Abstract—Hardware Trojan horses have become a troublesome challenge for security-sensitive integrated circuits. As one important categorization, the carrier of wireless-leakage hardware Trojan horse is radio wave, bypassed protective isolation equipment, such as traditional firewall. Even if no networking, it can also works, therefore more devilishness. This paper design a wireless-leakage hardware Trojan horse with Spartan-3E FPGA, which can pass system sensitive information to outside device with wireless radio signal by common pins, and the signals can be received by simple radios. Experimental results show that, a simple radio can receive the signal emitted by the hardware Trojan horse when their distance is more the 30 meters without any holdbacks. We also present a detection method and some defense suggestions.

Keywords— hardware trojan horse; covert channels; keys; encryption

I. INTRODUCTION

Hardware Trojan horses adhere and modify the design of hardware chip to change system functions [1], destroy system performance or reveal system sensitive information, such as the key of encryption chip. Compared with software Trojan horses, hardware Trojan horses are well-designed viciously to modify the hardware circuits [2], therefore they are more difficult to detect and defense, and more dangerous. According to security incidents in recent years, it has not been enough attention.

In order to grasp the working principle and detection method of hardware Trojan horses, this paper designed design a wireless-leakage hardware Trojan horse with Spartan-3E FPGA after deeply researching the current work of hardware Trojan horses. It can pass system sensitive information to outside device with wireless radio signal by common FPGA pins, and the signals can be received by simple radios. At the end of this paper, we present a detection method of such Trojan horses and show some defense suggestions of key devices.

II. RELATED WORK

In order to show the harmfulness of hardware Trojan horse, we give two real examples where hardware Trojan horses were found when transmitting unauthorized information with covert channels. In the first examples, Seagate external hard disks were found to have a wireless-leakage hardware Trojan horse that transmit user information to a remote device by radio signals [6]. In the second examples, some people reported that Vodafone routers in Greece were modified to allow spying phone conversation of the prime minister and other officials [5].

The above-mentioned finding indicates that, hardware Trojan horses well-designed viciously by attackers are dangerous and more difficult to detect and defense. However, Wireless-leakage problems involuntarily induced by designers are equally dangerous. It would be interesting to cite two generally known examples as following. In 1985, Wim-Van Eck presented the principle of video signal leakage and recovery, and used a modified black and white television set to recovery the information of computer display units [3]. In additions, a British capital intelligence agent, named Wright, exposed how to get the information sent by French diplomats. Firstly, he tried to crack the encryption system, but failed. However, Wright and his assistants found weak radio signals emitted by the device. In-depth analysis found that it is electromagnetic signal emitted by the cryptographic system, and restoring the signal can get the text without encrypted easily [4].

III. HARDWARE TROJAN ARCHITECTURE

In this section, we present a wireless-leakage hardware Trojan horse architecture, which can pass system sensitive information to outside device with wireless RF signal by common pins, and the signals can be received by simple radios. The core idea of this architecture is to construct the covert channel by tampering with the redundant resource (such as logical gates, placement and routing) of the FPGA chip, and achieve the purpose of important information disclosure (such as input date, secret keys, status registers) under the presets-conditions. It is parasitic on the normal circuit of encryption chip, and monitors the secret key, modulate it into specific RF signal, and transmit the signal through an FPGA pin.

Firstly, the hardware Trojan horse completes the triggering control by monitoring the input bus and the working state of the encryption chip. Then, it code the sensitive information according to the classical permutation algorithm, a single pulse represents “0” and two continuous pulses represents “1”, and modulate it into specific RF signal. Finally, it transmits the information through a FPGA pin. The RF signal can be received by a simple radio in a specific frequency band. The receiver can clearly hear the sound of “Di” or “Di Di”.

© 2016. The authors - Published by Atlantis Press
Figure I shows the logical framework of wireless-leakage hardware Trojan horse presented by this paper. In addition to the target encryption circuit, it also includes four modules, controller, clock generator, signal modulator and RF emitter, respectively. The controller is composed of signal control module and frequency division module, which is used to control the trigger condition and the transmission rate of the leaked information, i.e. secret keys. When the trigger control signal Ctrl_in is “true”, the controller generates one single pulse if the current bit of secret keys Key_in is “0”, and the controller generates two continuous pulses if the current bit of secret keys Key_in is “1”. The clock generator inputs the 50MHz system clock of the given FPGA development board, and outputs a specific frequency band clock between 80MHz and 120MHz. The signal modulator module is responsible for modulating the controller output signal to the carrier signal generated by the clock generator. The RF emitter is responsible for transmitting the output of signal modulator to the FPGA pin.

IV. SIMULATION VERIFICATION

The wireless-leakage hardware Trojan horse presented in the upper section is designed and implemented in a Spartan-3E FPGA board. This section describes some details of the implementation.

A. Trigger Module

The trigger module uses a time bomb or sequence detection to trigger the Trojan horse. When the trigger condition is satisfied, the enable signal of the Trojan horse can be successfully activated. Under such circumstances, the Trojan horse change its state from standby to activeness, and start sending secret key one bit by one bit. Whether the trigger signal is activated, the encryption chip with Trojan horse works normally.

B. Function Logical

In clock generator, half frequency and doubling frequency circuits of the system clock are designed. The half frequencies are implemented by two frequency counter, which can also be used to control the transmission rate and signal characterization. The doubling frequency are implemented by calling the clock management unit, DCM or PLL, which can also be used to modulate the outgoing data into signals. It is worth mentioning that its coding method is the classical permutation cipher algorithm, a single pulse represents “0” and two continuous pulses represents “1”. Moreover, we choose a tube feet with the ground wire as the transmitting antenna.

C. Simulation Result

The wireless-leakage hardware Trojan horse is simulated by Modelsim software tool. Figure II shows the simulation result. Among them, Key_in represents under sent information, i.e. secret keys. According to the system clock, clock generator module output three pulses, pulse1p5, pulse3 and pulse6, respectively. The combinational logic of Key_in, pulse1p5, pulse3 and pulse6 generate the pulse data_mid. The RF emitter modulates data_mid into data_out, and sends out. From figure II, it is can be seen that the high 6-bits of Key_in are “000100”, which respectively corresponding to the front 7 pulses. The “1” bit correspondences to the two continuous pulses, the other “0” bit correspondences to one pulse. This simulation results show that it works well.
D. Test Result

Its prototype system has been tested by Philips SBM120SLV radio. Under the preset band (FM 96.2MHz), the radio can send out the voice clearly. Of course, if receiving the signal by other radio under the preset band, you can also hear the sound. According to the sound, you can restore the secret key easily. When the distance between the radio and the prototype system is greater than 30 meters in the visibility conditions, the radio can also receive the RF signal properly. This test result shows that the prototype system works well.

V. DETECTION METHOD

Due to a wide variety of types, functions, implementation levels, and high covertness, it is difficult to detect hardware Trojan horses. The unknown trigger method of hardware Trojan horse greatly increases the difficulty of detection. Mature universal detection method has not yet appeared. However, we can build a detection system for wireless-leakage hardware Trojan horse according to the ultimate way of wireless leakage.

A. Detection System and Result

Figure III shows architecture of the detection system for wireless-leakage hardware Trojan horses. It is composed of three parts: HackRF One data acquisition card, GQRX display and GnuRadio decision maker. HackRF One is software defined radio platform from an open source hardware project, and HackRF One data acquisition card is responsible for collecting radio signals of under-test system. GQRX can visually display radio signals collected by HackRF One. GnuRadio decision maker analyses the radio signals to find out the abnormal signal which sends out by wireless-leakage hardware Trojan horses.

Figure IV shows the physical system of the detection system. The notebook runs GQRX display and GnuRadio decision maker, and its screen show the detection result by GQRX display. It is obviously that there are strong abnormal signals in the vicinity of 96.2MHz, and the abnormal signals changes over time with a certain rule, i.e., either 1 strong signal appears or 2 consecutive strong signals. This detection result show that the detection system works well.
VI. CONCLUSION

Hardware Trojan horses adhere and modify the design of hardware chip to change system functions, destroy system performance or reveal system sensitive information, such as the key of encryption chip. The carrier of wireless-leakage hardware Trojan horse is radio wave, bypassed protective isolation equipment, such as traditional firewall. Even if no networking, it can also works, therefore more devilishness. This paper design a wireless-leakage hardware Trojan horse with Spartan-3E FPGA, which can pass system sensitive information to outside device with wireless radio signal by common pins, and the signals can be received by simple radios. Experimental results show that, a simple radio can receive the signal emitted by the hardware Trojan horse when their distance is more the 30 meters without any holdbacks. We also present a detection method which is composed of three parts: HackRF One data acquisition card, GQRX display and GnuRadio decision maker. It is recommended to take the three safeguard procedures: Design special detection system, Take strict electromagnetic shielding measures, and Combine with computer defense tools to establish protection system.

ACKNOWLEDGMENT

This work was supported by Natural Science Foundation of China (Grant No. 61303061) and State Key Laboratory of high performance computing (Grant No.201513-01).

REFERENCES


