Research on Electromagnetic Side-channel Signal Extraction for Mobile Device PCM-9589F Multi-COM

Xiao-yang Hu^{1, a}, Kai-yan Chen¹, Yang Zhang¹, Dong-xin Guo¹ and Yan-hai Wei¹

¹Shijiazhuang campus of the Army Engineering University, Equipment Simulation Training Center, Shijiazhuang, China

Abstract. The portability and various functions of mobile devices enable them to go deep into people's study, work and life. While it is convenient for people, mobile devices contain a large number of user's private information, such as the user's personal property information, identity information and even the confidential information of enterprise etc. Side-channel attack is currently one of the most effective ways to steal private information of cryptographic devices thus the threat to mobile devices can be imagined. In this paper, the electromagnetic side-channel attack based on AES encryption algorithm on mobile device—PCM-9589F Multi-COM Board is studied. A new signal acquisition platform is designed, which solves the problem that the difficulty in locating the side-channel electromagnetic leakage signal of the mobile devices. In addition, using the time-frequency analysis and filter technology, we extract the encryption features of AES on PCM-9589F Multi-COM Board.

1 Introduction

Side-channel attack can make use of the physical leakage information of cryptographic devices that executing the encryption algorithm, which can obtain the specific encryption features of the cryptographic devices and crack the encryption key[1]. In traditional side-channel attack, it mainly focuses on small embedded devices such as smart cards, RFID tags, FPGA and microcontrollers. With the continuous development of mobile devices, people turn their eyes to mobile devices. The internal data protection mechanism of mobile devices only reduces the possibility of data leakage at the logical level. In theory, this protection mechanism cannot resist the threat of side-channel attack effectively. On the basis of traditional electromagnetic side-channel attacks, this paper turns to the mobile device—PCM-9589F Multi-COM Board (Figure 1). PCM-9589F Multi-COM Board is also called Atom main board, using Intel Atom N270 CPU, the front bus frequency is 533 MHz, with Intel 945GSE chip group. In this paper, it focuses on the problem that it is difficult to locate in the side-channel leakage signal of the mobile devices, and the signal is disturbed by other internal components of the system so that the encryption features cannot be extracted.

Figure 1. PCM-9589F Multi-COM Board.

2 Platform Construction

Compared with traditional small embedded devices, the structure of mobile devices is more complex. In the attack on mobile devices, the leakage signal produced by all the running programs in the system makes up the side-channel leakage signal together of mobile devices. The encryption operations are hidden in the whole system's background applications, and the extraction of useful signal in the attack process is difficult. In this paper, a solution is proposed for the difficulty in signal extraction on mobile devices.

2.1 Analysis of problems

Similar to traditional side-channel attacks, the side-channel attack on mobile devices uses the physical leakage of the devices. However, the differences are as

^aCorresponding author: *Xiao-yang Hu 1060954514@qq.com

follows:

(1) Difference in the complexity of the leakage signal.

Unlike small embedded devices, the PCM-9589F Multi-COM Board is a highly integrated computer main board with complex structure, it contains a large number of components. The extracted leakage signal will be influenced by a large number of irrelevant signal, which are regarded as noise.

Let P_{total} be the measured physical leakage signal of a mobile device. Then, the whole leakage signal can be separated into several components such as an operation-dependent part P_{op} , a data-dependent part P_{data} , noise from the environment P_{env} , and noise caused by the measurement devices P_{dev} (such as the noise generated by digitizing process of the oscilloscope, and the noise of the electromagnetic probe, etc). P_{total} can therefore be modeled as a sum of those components, it can be expressed as:

$$P_{total} = P_{op} + P_{data} + P_{env} + P_{dev} \quad (1)$$

In the traditional side-channel attacks on small embedded devices, such as microcontroller as an example, it contains only the leakage signal of the device executing encryption operations. For mobile devices, as the system runs, the CPU runs fast and continues to process a large number of applications, and the components are interfered with each other at work. Therefore, the leakage signal related to the encryption operations and the leakage signal produced by a large number of other system components consisted of P_{op} together. Let P_{oth} be the leakage signal depended on the other internal components of mobile devices. Therefore, the form (1) can also be rewritten as:

$$P_{total} = P_{enc} + P_{oth} + P_{data} + P_{env} + P_{dev} \quad (2)$$

(2) Difference in the way of trigger signal generated.

The small embedded devices can make the clock edge change by setting the device's pins, triggering the oscilloscope to collect the leakage signal when the target device performs encryption operations[2]. If a AT89C52 microcontroller is used as the target device, the P1.1 pin can be directly placed 0 by the internal control program to produce a clock down edge and trigger the oscilloscope sampling. In addition, trigger signal can also be generated in other small embedded devices by using related protocols. There is no similar structure for the PCM-9589F Multi-COM Board, so new methods in triggering oscilloscope sampling are needed (seen in Section 2.2).

(3) Difference in signal processing methods

Compared with the traditional side-channel attacks, the signal component of the side-channel leakage of the PCM-9589F Multi-COM Board is more complex when performing the encryption operations. Therefore, the time-frequency analysis technique is used in the signal processing to determine the frequency range of the side-channel leakage signal related to the encryption operations and the filter technique is used to remove the noise generated by other components of the system and

external environment[3].

2.2 Proposal of experimental scheme

The experiment setup of this paper is mainly composed of the following modules:

(1) Control module: Control computer (hereinafter referred to as the host) with LabView signal acquisition software. It is used to control transfer data between host and target device, and to control the sampling of the oscilloscope. A LabView signal acquisition software is set up in the host computer to configure the sampling parameters of the oscilloscope.

(2) Target module: PCM-9589F Multi-COM Board. Attack object and the carrier of encryption algorithm.

(3) Trigger module: Composed of host and the AT89C52 microcontroller, which is used to generate trigger signal and control oscilloscope sampling. The pins of AT89C52 microcontroller is set up by the host through serial port to generate trigger signal and control oscilloscope sampling.

(4) Data acquisition module: Including Tektronix DPO4032 digital oscilloscope, electromagnetic probe (Langer RF-R 400-1), PA303 Amplifier, AT89C52 microcontroller.

In order to obtain the electromagnetic radiation signal of the target device in the process of encryption, the Tektronix DPO4032 digital oscilloscope with the PA303 Amplifier and the Langer RF-R 400-1 electromagnetic probe are used as the signal acquisition equipment. As the PCM-9589F Multi-COM Board can not generate trigger signal by itself, the AT89C52 microcontroller is added with the host as the trigger signal generation module together.

The schematic diagram of designed platform for attack on PCM-9589F Multi-COM Board is shown in Figure 2.

Figure 2. The schematic diagram of attack platform.

As shown in Figure 2, the host is connected to the target device, the microcontroller and the oscilloscope through the serial port, with the LabView signal acquisition software built inside, sending the plaintext to the target device and configuring the sampling parameters of the oscilloscope. When the parameter configuration is completed, the oscilloscope doesn't start sample until the trigger signal arriving. Following the

principle "first triggering and post encrypting", when the target device receives a set of plaintext sent by the host through the serial port1, the host sends the commands through serial port2 to the microcontroller to generate a trigger signal and trigger the oscilloscope to sample. After that, the target device begins to encrypt the plaintext. After sampling, the traces are sent to the host through the serial port1 for further analysis.

It is important to note that because the data processing speed of the serial port is far less than the CPU data processing speed of the target board, the Sleep command is needed to make the target device wait for a certain time until the oscilloscope receives the trigger signal, the encryption for plaintext is then started[4]. In addition, the correlation time procedure is used to determine the time period of the target device executing the encryption algorithm to determine the sampling length of the oscilloscope. The platform mainly uses serial communication technology to realize the function of each module. The advantage is that the trigger signal is controlled by the host directly. It is not dependent on the target device itself, and it is suitable for all mobile devices. Therefore, to a certain extent, the platform is universal for the side-channel leakage signal acquisition of mobile devices.

3 Attacking Experiment

In this section, the experiment of the side-channel attack on the PCM-9589F Multi-COM Board is executed using the designed platform as Figure 2, and the electromagnetic side-channel leakage signal extraction of the target device running AES encryption algorithm is carried out. Figure 3 shows the real attack platform.

Figure 3. Real attack platform.

Using the setup as Figure 3, the electromagnetic leakage signal traces of PCM-9589F running AES encryption algorithm are collected.

Figure 4. The raw traces obtained by the experimental setup.

As seen in Figure 4, the quality of the raw signal traces is poor, and it is almost impossible to distinguish the features of AES encryption features, so the traces need to be further processed.

3.1 Side-channel leakage signal processing

From Figure 4, it can be observed that in the time domain, the useful-signal is interfered by a large number of noise, the encryption features of AES cannot be extracted. Therefore, we use MATLAB software to carry out short-time Fourier Transform (STFT)[5,6] to carry out the spectrum analysis. In order to find out the frequency range of the electromagnetic leakage signal that depended on the AES encryption operations, we use the filter technique to remove the interference of the noise. In the experiment, the raw signal traces are processed with twice STFT transformation and filter respectively. Short-time Fourier Transform(STFT) is computed as:

$$\text{STFT}_z(t, f) = \int_{-\infty}^{\infty} [z(u)g^*(u-t)]e^{-2\pi f u j} du \quad (3)$$

In formula (3), $z(t)$ is the raw traces and $g(t)$ is a window function. In order to facilitate the processing of computer, it is also discretized as:

$$\text{STFT}_z(m, n) = \sum_{k=-\infty}^{\infty} z(k)g^*(kT-mT)e^{-2\pi(nF)kj} \quad (4)$$

Figure 5 shows the energy spectrogram of the raw traces after the first short-time Fourier Transform.

Figure 5. The spectrum of the traces after first STFT transformation.

As shown in Figure 5, the transverse axis is the time axis (second) and the longitudinal axis is the frequency axis (Hz). The stripe with different color depth is the energy traces corresponding to each frequency point of the traces. The deeper the color, the greater the amplitude of the traces are. The energy traces stripe of encryption operations produced by the target device and the other energy stripes of noise can be observed from the diagram. After analysis, the energy traces stripe produced by the AES encryption operations is labeled as in the graph, so the pass-band range of the digital filter is 800MHz~850MHz. Other energy traces are the electromagnetic radiation signal and random noise generated by other components of the target device. After selecting the pass-band range of the filter, the band-pass filter is designed to filter out the noise in the target device system[7].

3.2 Filter processing for raw traces

Because of the complex structure and a lot of components of mobile devices, the side-channel leakage traces are greatly disturbed by noise. Thus, twice of filtering techniques are used in the experiment. In section 3.1, it shows that the pass-band frequency of the first digital filter is 800MHz~850MHz. The traces after the first filter are shown in Figure 6. After the first filter, some noise signal are reduced, but the complete AES encryption features cannot be seen yet, so the second filter is needed so that the AES encryption features can be observed more intuitively in lower frequency band.

Figure 6. Traces after first filter.

On the basis of the first filter, the traces are analyzed again, and the spectrum diagram after second analysis of the traces is shown in Figure 7. At this time, it can be clearly observed that the range of the frequency of the AES encryption traces is 50MHz~80MHz, so the frequency-range of the second filter is 50MHz~80MHz.

Figure 7. The spectrum of the traces after second STFT transformation.

After the second filter, the traces are shown in Figure 8. The whole AES ten rounds encryption features can be clearly seen this time. Because the tenth round encryption lacks the column mixing transformation, the encryption time is slightly shorter than the other 9 rounds encryption time.

Figure 8. Traces after twice filter.

4 Conclusion

On the basis of the signal extraction methods in traditional side-channel attacks, this paper uses serial port communication technology to build a signal acquisition platform for extracting the side-channel leakage signal of mobile device PCM-9589F Multi-COM Board, which solves the problem of signal extraction of the mobile devices. The advantage of this platform is that the design of the platform is applicable to the side-channel leakage signal acquisition of any mobile devices. In this paper, the trigger signal is produced by using the host computer to control the microcontroller directly, triggering the oscilloscope sampling and solving the problem that the mobile devices cannot generate the trigger signal by themselves. And we use the filter technique to reduce the noise produced by a lot of components in mobile devices or other external noise.

However, there are still some problems to be solved in the study. For example, due to the working frequency of CPU is much higher than the data transmission rate of the serial port, the target device don't encrypt until the oscilloscope triggered, the time for that is difficult to control. Therefore, the method proposed in this paper can only guarantee the oscilloscope to collect the integrated encryption process but it cannot locate the specific encrypt operation precisely. Further research is needed in this regard.

References

1. Kocher, Paul C., Joshua M. Jaffe, Benjamin C. Jun, and Inc Cryptography Research. (2009)
2. Amoth, Dough. "Intel details next-generation 'Pine Trail' Atom platform, intros updated 'Moblin' UI |TechCrunch." TechCrunch. N.p., n.d. Web. 31 Mar. (2013)
3. Cangeloso, San. "Intel Silverthorne, Diamondville to hit the streets as Atom | Chips | Geek.com." Geek.com. N.p., n.d. Web. 31 Mar. (2013)
4. Aboukassimi D, Agoyan M, Freund L, et al. Electro-Magnetic analysis (EMA) of software AES on Java mobile phones.[J]. 1-6 (2011)
5. Goller G, Sigl G. Side Channel Attacks on Smart-phones and Embedded Devices Using Standard Radio Equipment[C]// Revised Selected Papers of the, International Workshop on Constructive Side-Channel Analysis and Secure Design. Springer-Verlag New York, Inc. 255-270 (2015)
6. Nakano Y, Souissi Y, Nguyen R, et al. A Pre-processing Composition for Secret Key Recovery on Android Smartphone[C]// Ifip Wg 11.2 International Workshop on Information Security Theory and Practice. Securing the Internet of Things. Springer-Verlag New York, Inc. 76-91 (2014)
7. Oswald, David, and Christof Paar. "Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World." Cryptographic hardware and embedded systems-CHES 2011 13th

international workshop, Nara, Japan, September
28-October 1, 2011 : proceedings. Heidelberg:

Springer.(2011)