Safeguarding Unmanned Aerial Vehicles Against Side Channel Analysis Via Motor Noise Injection

Timothy Radtke
Electrical and Computer Engineering Dept.
Marquette University
Milwaukee, WI, USA
timothy.radtke@marquette.edu

Cristinel Ababei
Electrical and Computer Engineering Dept.
Marquette Universty
Milwaukee, WI, USA
cristinel.ababei@marquette.edu

***Abstract*—We first investigate the efficacy of side channel analysis (SCA) based attacks to recover the encryption key from an unmanned aerial vehicle (UAV). We then propose a method based on noise injection to safeguard against this type of attack. The proposed noise injection method is unique because it prioritizes low power consumption and uses as a noise source the motors of the UAV system. The effectiveness of the proposed method is demonstrated through experiments on a real quadcopter. It is found that when noise injection is not applied, the encryption key can be recovered through correlation power analysis. In contrast, the same key is not recoverable when the proposed noise injection method is applied. The implemented solution is efficient and does not negatively effect the flight stability or control of the UAV because its execution time overhead is negligible inside the control loop. In addition, it consumes a negligible amount of power. These results demonstrate that mitigation of SCA attacks without expanding the complexity or negatively effecting the flight operations of drones is achievable.**

***Index Terms*—unmanned aerial vehicle, UAV security, side channel analysis, SCA mitigation, power analysis**

I. Introduction

Recently, the popularity of unmanned aerial vehicles (UAVs) or drones has increased in many application domains, including public safety, search and rescue, traffic monitoring, communications deployment, and defense [1]. Increasingly, UAVs are becoming an integral part of the internet of things (IoT) in both the public and military sectors. This development has resulted also in an increase in the threat from maligned actors. These attackers break into these devices to steal sensitive information or to disrupt the UAVs mission, and this can result in harm to public safety and security. Because a lot of these attacks and their countermeasures have been software based mainly, the inherent hardware vulnerabilities present in UAVs have received less attention [2]. For example, after Iran shot down an US RQ-4A Global Hawk drone in 2019, it was reported that hardware analysis of the UAV's control systems was leveraged to gain intelligence [3], [4]. This attack demonstrates that malicious actors can also use hardware in addition to software vulnerabilities of UAVs. Therefore, there is a growing need for hardware based security solutions for embedded systems, especially those found in the connected IoT devices such as UAVs. The safeguarding of these devices against hardware based security attacks, such as side channel analysis, is critical to the success and safety of these technologies.

II. Related Work and Contribution

Research on UAV hardware security is relatively new, and has focused on the application of physically unclonable functions (PUFs) to prevent backdoor access at the silicon level after chip manufacturing. Using side channel analysis (SCA) techniques on UAV embedded systems was investigated in the study from [5]. The authors provided a trusted hardware framework to protect against sophisticated hardware side channel attacks that would go unnoticed by the UAV's control system. The proposed framework provides protection against cyber-physical attacks such as attempts to spoof or corrupt various sensor readings. One such critical sensor is the inertial measurement unit (IMU): disrupting this sensor could lead to loss of stability and cause the drone to crash. Such attacks can result into hijacking the UAV's flight dynamics and giving control to the attacker. Similarly, when global positioning system (GPS) signals are disturbed, the UAV can be moved into non-intended airspace. Similar research and experimentation was reported in other studies [6], [7]. These studies focused on adding additional trusted hardware and processing cores to the original hardware, thereby increasing its complexity and power consumption.

Techniques in side channel analysis or attack for extraction of encryption keys have advanced over the past several years. Differential power analysis (DPA) and correlation power analysis were successfully applied to various microarchitectures, including those often found within the primary control system of a UAV. Consequently, various commercially available tools were developed to automate the collection and analysis of the power traces required for side channel attacks. Research in chip power management, such as the work in [8] has provided researchers with the tools and methods necessary to effectively apply the differential power technique to a wide variety of IoT devices. Additionally, the work in [9] demonstrated the ability extract an AES key from a military-grade field programmable gate array (FPGA) using DPA. In contrast, the research into methods to counter SCA and differential or correlation power methods is in its infancy. Studies in [10], [11] demonstrate the viability of using electrical noise, either generated or injected,

to prevent successful SCA attacks. These noise techniques are designed to reduce the signal to noise ratio of the power signal, or intelligently mask the encryption power signature through attenuation. In practice, these techniques have been studied on FPGA development boards or specialized application specific integrated circuits (ASICs) such as hardware security modules. Hence, the study of these techniques on general-purpose microprocessors and microcontrollers commonly found in UAVs is rather limited.

In this paper, we make two main contributions: 1) We demonstrate on real hardware the security threat that side channel analysis presents to UAV platforms and 2) We propose a solution that mitigates this threat. This solution prevents UAVs from being attacked by correlation power analysis, differential power analysis, and other similar power analysis techniques. Additionally, the solution is power conscious because it is important for any proposed solution to not negatively impact flight time of the aircraft. Thus, we provide an effective low power method to prevent side channel analysis and increase security of UAVs embedded control systems.

III. Background Information

In this section, we discuss various terms and concepts related to UAVs, including basics of side channel analysis (SCA) and correlation power analysis (CPA).

A. UAV Topology

One of the most popular UAV topologies in practice is the one that uses four motors. Such drones are also commonly referred to as quadcopters. The block diagram of a quadcopter is shown in Fig. 1, and it is the one we use for our experiments later on. The quadcopter is controlled via a standard handheld radio transceiver. The flight control algorithm includes auto leveling control techniques for stability during flight. To assist the auto leveling algorithm, an inertial measurement unit (IMU) is used to determine the roll, pitch, and yaw of the aircraft. Fig. 1 depicts the MPU6050 IMU, the electronic speed controllers (ESCs) that drive the brushless direct current (BLDC) motors, and the control hub implemented with a microcontroller, which runs the flight control algorithm. The quadcopter is powered by a lithium polymer (LiPo) battery, which provides power for approximately 20 minutes of flight time. In addition to auto leveling, the UAV is capable of encrypting data stored in the EEPROM of the ATMega328 microcontroller using 128 bit advanced encryption standard (AES-128) in the cipher block chaining (CBC) mode. For the purpose of the experiments in this paper, it is assumed that the data stored represents a mission plan - therefore of crucial importance - that is communicated to other UAVs during a surveillance operation.

B. Side Channel Analysis

Side channel analysis (SCA) typically takes a power analysis form. However, there is another form called electromagnetic analysis. Instead of measuring the current consumed by a microcontroller, this technique measures the electromagnetic radiation as a magnetic or electrical field [9]. To perform power analysis, the current of the device in question is typically measured with a shunt resistor on the primary power line feeding the microcontroller. Then, power consumption values reveal the number of bits changing states, in turn which provides information about the instructions being executed [9], [12]. Correlation power analysis (CPA) is a form of SCA that attempts to correlate observed power consumption data with expected consumption during specific events: in this case, the output of the *SBOX operation* of the AES-128 algorithm [8], [12]. Rather than brute forcing the entire 16 bytes of the key, for each SBOX round, one only needs to brute force one byte of the key at a time, which is trivial on modern processors.

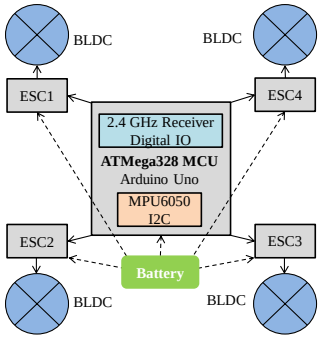

Fig. 1. System level block diagram of the UAV quadcopter used in this work.

IV. Proposed Safeguarding Method

In this section, we describe the proposed method, which is intended to prevent SCA attacks and to increase the hardware security posture of an UAV. First, we demonstrate the use of CPA for AES key extraction. After demonstrating the AES key can be recovered (i.e., stolen) using CPA, we examine in detail the electrical noise generated during BLDC startup. It is precisely this noise that we propose to use as the *entropy source* to inject noise into the power supply line of the UAV, thereby masking the power signature of the cryptographic operation. The injection of random noise is experimentally tested by re-applying the original attack technique to steal the AES key and observing its failure to recover the key. These experiments are conducted on a real quadcopter and successfully validate the effectiveness of the proposed method.

A. AES Key Theft Using Side Channel Analysis

For a CPA attack to be successful, a collection of power traces and their corresponding plaintexts (i.e., unencrypted information) is required. After gathering this information, a power hypothesis is built for each of the 256 possible values of the key byte [12]. Then, a modified version of Pearson's correlation coefficient is used to determine the most likely key byte by computing the coefficient between the power hypothesis and the measured power trace. The alternate form, described by eq. (1) below, is used to speed up computation because it allows summation of one trace at a time without re-summing all of the past data [13].

$$r_{i,j} = \frac{D\sum_{d=1}^{D} h_{d,i}t_{d,j} - \sum_{d=1}^{D} h_{d,i}\sum_{d=1}^{D} t_{d,j}}{\sqrt{\left(\left(\sum_{d=1}^{D} h_{d,i}\right)^2 - D\sum_{d=1}^{D} h_{d,i}^2\right)\left(\left(\sum_{d=1}^{D} t_{d,j}\right)^2 - D\sum_{d=1}^{D} t_{d,j}^2\right)}} \quad (1)$$

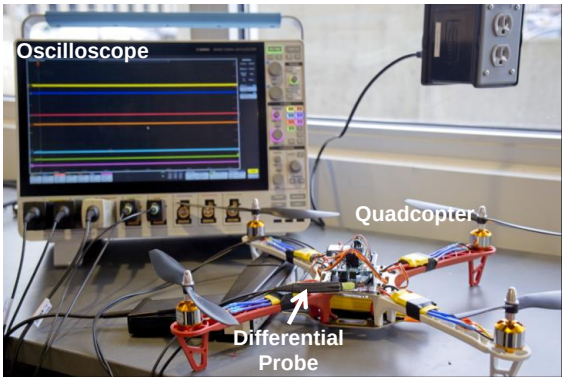

Fig. 2. Photograph of the experimental setup with the in-house built quadcopter.

Where D is a set containing power traces, where each trace includes T data points. $t_{d,j}$ is data point j in power trace d and $h_{d,i}$ is the power estimate for trace d assuming the key byte is i. $r_{i,j}$ is the correlation coefficient for subkey i at the point j [13].

All practical UAVs communicate with the outside world. Therefore, implicitly there exists a communication mechanism or interface to request encryption from the UAV. Hence, an attacker only needs to request encryption of enough messages and capture the power traces of each encryption byte, thereby obtaining all the pieces needed to then launch a CPA attack. To demonstrate such an attack, we instrument our in-house built quadcopter whose topology was discussed in section III and which is shown in Fig. 2. The main flight control algorithm is run on the ATMega328 microcontroller of the Arduino Uno platform. To capture power traces, a 10 Ohm resistor is soldered inline with the power supply of the microcontroller. Then, the voltage across the resistor is measured with a 500 MHz differential probe, which is connected to a Tektronix MSO58 oscilloscope. Having known the resistance value and the voltage drop across it (thus the current through the resistor as well), we can readily calculate the power trace.

To effectively execute the attack, it is very important to automate the delivery of plaintexts and control of the scope to capture and save the traces. For this purpose, a Python program was written to setup the oscilloscope, deliver the plaintexts, capture the power trace, and save it as a CSV file to a disk drive attached to the scope. Once all traces are gathered, another Python program cleans and prepares the CSV files gathered from the oscilloscope. These files are finally used as input into a third Python program that implements the CPA algorithm and outputs each byte of the key as it is found.

B. Motor Noise Profile

Having a good source of entropy is imperative to a true random number generator, and electrical noise can be an excellent source of entropy [14]. During the startup operation of a brushless DC motor, electrical noise is generated, which impacts the current profile of the motor. An example of this noise is shown on the oscilloscope screenshot from Fig. 3, collected during our experiments. To confirm this noise can

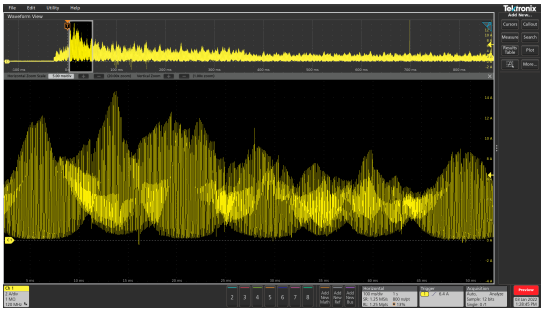

Fig. 3. Oscilloscope screenshot showing the motor current during startup and takeoff operation of the quadcopter.

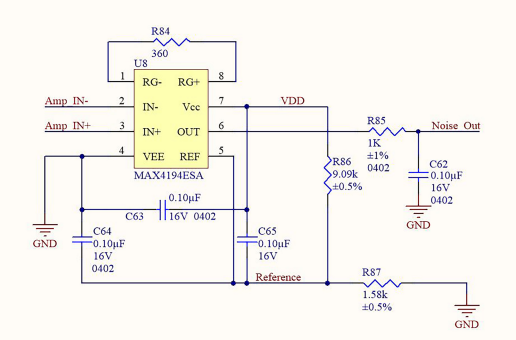

Fig. 4. Schematic diagram of the instrumentation amplifier circuit, which is used for injecting noise into the power supply of the microcontroller.

provide a good source of entropy to the UAV's control system, the data from the current plot gathered by the scope is saved and run through entropy statistical tests. Specifically, we chose to use Dieharder tests [15] to test the randomness of the noise data because they include tests from the NIST statistical suite.

C. Noise Injection to Counter Side Channel Analysis

Once confirmed as an excellent source of entropy, the motor noise is injected into the main power line of the microcontroller. Such noise will disrupt the success of the CPA attack by creating an environment where no power hypothesis will strongly correlate with the trace captured from the UAV. To inject the noise, a shunt resistor is placed inline with the power path feeding the ESC and a differential amplifier measures the voltage drop across this resistor. Fig. 4 depicts the differential amplifier circuit implemented. The input nets *Amp IN-* and *Amp IN+* in Fig. 4 are connected to the sides of the shunt resistor and the output net, *Noise Out*, is connected through a diode to the power rail of the Arduino Uno microcontroller board. To increase the effectiveness of the noise, the gain of the amplifier is set to approximately 200 via the feedback resistor R84; this value was found empirically to provide good results.

V. Experimental Results

A. Successful SCA Attack

Using the technique described in section IV-A, we first collected 350 power traces from the quadcopter using 350 unique plaintexts. Fig. 5 is an example trace gathered during this attack. Gathering all 350 traces from the UAV takes approximately 10 minutes, at which point, the UAV could be

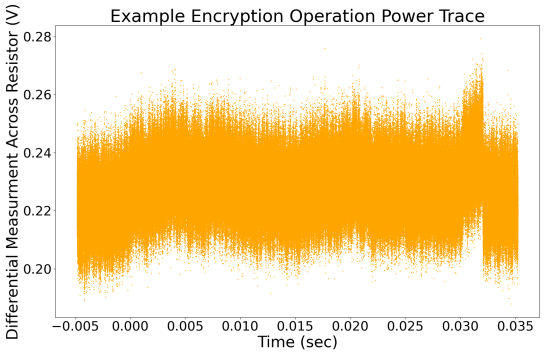

Fig. 5. Example trace collected using the differential probe and oscilloscope during the SCA attack.

returned to the control of the original operator minimizing the chance of notice it is missing for the duration of the attack procedure. After gathering the power traces, the aforementioned Python programs are run to process the power trace data and to recover the key. The experiment was conducted three times for three different random keys. In the first two runs of the experiment, the first two keys were successfully recovered. The third key required an additional 100 power traces to fully recover it; hence, 500 traces is recommended to recover any random key.

B. Safeguarding via Noise Injection

Having shown CPA as an effective attack to steal the AES key stored inside the quadcopter, motor noise is measured for each of the four BLDCs as discussed in section IV-B. Fig. 3 provides an example plot from these measurements. These motor noise measurements are run through the Dieharder test suite and only three of the 114 tests were reported weak - which is an excellent result. The tests reported weak were diehard sums, the second instance of diehard runs, and the second instance of rgb lagged sums. This result demonstrates the capability of electrical noise generated by the motors to serve as a good source of entropy, and thus of effectively masking the power signature of an encryption operation. Moreover, the circuit implemented and described in Fig. 4 to inject noise into the power rail of the UAV microcontroller only consumes 100 uA, which makes for the proposed solution to be truly low power. Furthermore, the extra noise on the power rail has no observable negative effects on the flight capability of the quadcopter nor the ability to auto-level.

Once the noise injection circuit was implemented and integrated into the existing hardware of the quadcopter, we conducted the initial three experiments from the previous subsection for the same AES keys. For each experiment, 500 power traces were captured. The data acquisition took approximately 15 minutes to complete. Similarly to the initial experiments, traces were processed and the CPA algorithm was used to attempt key recovery. Despite using the same procedure as in the initial experiment, the CPA attack fails to recover the key when the noise injection technique is applied. The calculated correlation values for each key value stayed at or below 0.4 and no power hypothesis creates a clear lead as it was observed during the initial experiment. Hence, injecting electrical noise generated by the motors during startup and takeoff is verified as an effective countermeasure to side channel analysis.

VI. Conclusion

As UAVs become increasingly popular in many public and military applications, so does their security, especially against SCA attacks. To counteract such attacks, we proposed a method that uses injection of noise from the UAV motors into the power rail of the microcontroller, which runs the flight control algorithm and stores critical information, such as AES encryption keys. Experiments on an in-house built quadcopter demonstrated the vulnerability of the unprotected UAV system as well as the effectiveness of the proposed method in safeguarding the UAV against SCA attacks. As future work, it would be interesting to investigate whether the motor noise evaluated in this work can be used as an entropy source for a firmware solution to complement the hardware one presented and thus to further increase resilience against power analysis attacks. This idea could be implemented by reading the *Noise Out* value in Fig. 4 by an analog to digital converter, readily available in modern microcontrollers. The converted digital value could then be used as a random number to insert stall operations into the AES algorithm causing further disruption of the power signature during encryption.

References

[1] "Government accountability office report: Technology assessment, internet of things: Status, implications of an increasingly connected world," May 16, 2017.

[2] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, "Uav iot framework views and challenges: Towards protecting drones as things," No. 4015, Sensors, November 2018.

[3] H. Sutton, "Iran rebuilds u.s. navy global hawk uav it shot down," July 2020.

[4] L. Newman, "The drone iran shot down was a 220 million dollar surveillance monster," June 20 2019.

[5] F. Fei, Z. Tu, R. Yu, T. Kim, X. Zhang, D. Xu, and X. Deng, "Cross-layer retrofitting of uavs against cyber-physical attacks," pp. 550–557, IEEE, May 2018.

[6] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting secure communication under uav smart attack with imperfect channel estimation," *IEEE Access*, vol. 6, pp. 76395–76401, 2018.

[7] J. McNeely, M. Hatfield, A. Hasan, and N. Jahan, "Detection of uav hijacking and malfunctions via variations in flight data statistics," pp. 1–8, IEEE, Oct. 2016.

[8] A. Singh, M. Dar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Exploiting on chip power management for side channel security," 2018.

[9] S. Skorobogatov and C. Woods, "In the blink of an eye: There goes you aes key," May 2012.

[10] A. Baylis, G. Stitt, and A. Gordon-Ross, "Overlay-based side-channel countermeasures: A case study on correlated noise generation," pp. 1308–1311, IEEE, Aug. 2017.

[11] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," pp. 62–67, IEEE, May 2017.

[12] U. Banerjee, L. Ho, and S. Koppula, "Power-based side-channel attack for aes key extraction on the atmega328 microcontroller." Online, 2015.

[13] C. O'Flynn, "Correlation power analysis."

[14] L. Gong, J. Zhang, H. Liu, L. Sang, and Y. Wang, "True random number generators using electrical noise," *IEEE Access*, vol. PP, pp. 1–1, 09 2019.

[15] R Core Team, *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria, 2021.