Demo: Detecting Illicit Drone Video Filming Using Cryptanalysis

Ben Nassi,[1] Raz Ben-Netanel,[1] Adi Shamir,[2] Yuval Elovici[1]
[1] Ben-Gurion University of the Negev, [2] Weizmann Institute of Science
nassib@post.bgu.ac.il, razx@post.bgu.ac.il, adi.shamir@weizmann.ac.il, and elovici@inter.net.il

Video 1 - https://youtu.be/4icQwducz68 **Video 2** - https://youtu.be/9PVaDpMsyQE

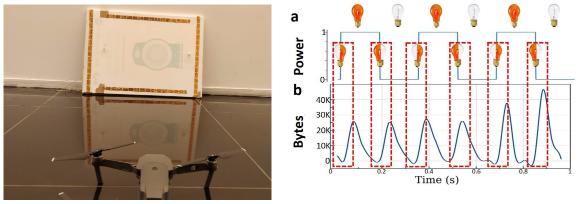

Fig. 1. Left: A drone placed in front of a whiteboard with an attached LED strip. Right: (a) the flickering LED strip that operates at 3 Hz creates (b) six bursts in the intercepted bitrate signal extracted from the drone.

***Abstract*—In this demo, we demonstrate that cryptanalysis can be used to determine whether a passing drone is used for spying, by analyzing the drone's encrypted video channel. We also show that a spying drone can be detected when the victim is located in a house or traveling in a car, with the use of a flickering light.**

IN an era in which drones are flying among us, a new question arises [1]: how can we determine whether a passing drone is being used by its operator for a legitimate purpose (e.g., delivering a pizza) or an illegitimate purpose (e.g., taking a peek at a person showering in his/her own house)? In this demo, we demonstrate that cryptanalysis can be used to determine whether a passing drone is used for spying, by analyzing the drone's encrypted video channel.

First, we show how the side effect of the H.264 video compression algorithm, the variable bitrate, can be utilized to detect whether a drone's camera is used to film an object, by analyzing the traffic of the video channel. To do this, we position a DJI Mavic Pro in front of a whiteboard with an attached LED strip connected to Arduino Uno (see Fig. 1). The LED strip is programmed to flicker at 3 Hz. We extract the bitrate signal by sniffing encrypted Wi-Fi packets sent from the drone to its controller using Airmon-ng.

We use the intercepted encrypted packets in order to extract a time series, using unencrypted metadata from each packet: (1) the packet arrival time, and (2) the size. Fig. 1 presents the results of this experiment. As can be seen, a 3 Hz flickering LED strip creates a 6 Hz phenomenon within the intercepted bitrate signal by producing six bursts per second. Each time the LED strip is turned on/off, a larger amount of data is sent from the drone, which is expressed as a burst of bytes in the time domain. Based on the results of this experiment, we conclude that by attaching a flicker to an object, we can detect whether a drone's camera is used to film the object, by analyzing the video channel, even if the traffic is encrypted.

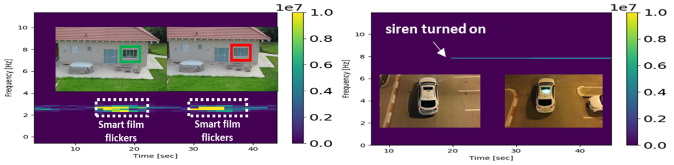

Fig. 2. spectrograms of the intercepted bitrate signal obtained from the intercepted bitrate signal when a drone was used to spy on the victim that was located in his house (left) and in his car (right).

Next, we demonstrate how a smart film attached to a window can be used to detect whether a drone is used to film a private house from a neighboring property. In this experiment, smart film (film that changes its state from transparent to mat and vice versa) that has been installed on a victim's living room window is used for flickering. A video of this experiment can been in the link above. Fig. 2 presents a spectrogram of the intercepted bitrate signal that was extracted during this experiment. The effect of the flickering film on the intercepted bitrate signal shows how a spying drone can be detected by a victim located in a house.

Finally, we demonstrate how a siren installed on top of a car can be used to detect whether a drone is used to film a subject while he/she is traveling in a car. A video of this experiment can been in the link above. Fig. 2 presents a spectrogram of the intercepted bitrate signal that was extracted during this experiment. The effect of the flickering siren on the intercepted bitrate signal shows how a spying drone can be detected by a victim traveling in a car.

The extended version of this paper can be found in [2], [3].

REFERENCES

[1] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "Sok: Security and privacy in the age of commercial drones," in *2021 2021 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, may 2021, pp. 73–90.

[2] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici, "Drones' cryptanalysis-smashing cryptography with a flicker," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1397–1414.

[3] R. Ben Netanel, B. Nassi, A. Shamir, and Y. Elovici, "Detecting spying drones," *IEEE Security Privacy*, vol. 19, no. 1, pp. 65–73, 2021.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021
25 February 2021, Virtual
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2021.23003
www.ndss-symposium.org