First method to detect illicit drone filming developed

January 15 2018

Credit: CC0 Public Domain

The first technique to detect a drone camera illicitly capturing video is revealed in a new study published by Ben-Gurion University of the Negev (BGU) and Weizmann Institute of Science cyber security

researchers. The study addresses increasing concerns about the proliferation of drone use for personal and business applications and how it is impinging on privacy and safety.

In a new paper, "Game of Drones - Detecting Captured Target from an Encrypted Video Stream," the researchers demonstrate techniques for detecting if a targeted subject or house is being recorded by a drone camera.

"The beauty of this research is that someone using only a laptop and an object that flickers can detect if someone is using a drone to spy on them," says Ben Nassi, a Ph.D. student in the BGU Department of Software and Information Systems Engineering and a researcher at the BGU Cyber Security Research Center (CSRC). "While it has been possible to detect a drone, now someone can also tell if it is recording a video of your location or something else."

In the first demo, researchers show how a privacy invasion against a house can be detected. They used smart film placed on a window and entered a few software commands on a laptop to access the encrypted video the drone operator sees, called the FPV channel. This enabled the researchers to demonstrate how they detect that a neighbor is using a DJI Mavic drone to capture images of his own home and then illicitly stream video of his neighbor's house, as well. Click here to watch a video of the demonstration.

In a second outdoor test, researchers demonstrate how an LED strip attached to a person wearing a white shirt can be used to detect targeted drone activity. When researchers flickered the LED lights on the cyber-shirt, it caused the FPV channel to send an "SOS" by modulating changes in data sent by the flickering lights.

"This research shatters the commonly held belief that using encryption to

secure the FPV channel prevents someone from knowing they are being tracked," Nassi says. "The secret behind our method is to force controlled physical changes to the captured target that influence the bitrate (data) transmitted on the FPV channel."

This method can be used on any laptop that runs Linux OS and does not require any sophisticated hacking or cryptographic breaking skills.

"Our findings may help thwart privacy invasion attacks that are becoming more common with increasing drone use," Nassi says. "This could have significant impact for the military and for consumers because a victim can now legally prove that a neighbor was invading their privacy."

In previous research, Nassi showed how a laser mounted to a DJI Inspire 1 drone can use malware installed on an isolated (air-gapped) network scanner. Click here to watch a video of this demonstration.

Provided by American Associates, Ben-Gurion University of the Negev

Citation: First method to detect illicit drone filming developed (2018, January 15) retrieved 20 March 2023 from https://phys.org/news/2018-01-method-illicit-drone.html