SPIES IN THE SKY

Israeli researchers develop a countersurveillance drone system

By Joe Charlaff

THE USE of drones for surveillance is no longer in the realm of science fiction. We are now in an era in which anyone with a drone equipped with a video camera can use it to invade a subject's privacy by streaming the subject in his/her private space over an encrypted first-person view (FPV) channel.

Experts suggested many methods to detect nearby drones, but they all suffer from the same shortcoming: they cannot identify exactly what is being captured, and therefore they fail to distinguish between the legitimate use of a drone (for example, using a drone to film a selfie from the air) and illegitimate use that invades someone's privacy (when the same operator uses the drone to stream the view into the window of his neighbor's apartment), a distinction that in some cases depends on the orientation of the drone's video camera rather than on the drone's location.

Drones have been used for photographing sensitive locations. One of the most notable concerns about UAS platforms stems from their potential to silently monitor and record their surroundings.

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.

Researchers have built a proof-of-concept system for countersurveillance against spy drones that demonstrates a clever, if not exactly simple, way to determine whether a certain person or object is under aerial surveillance.

They first generate a recognizable pattern on a subject – a window, say – someone might want to guard from potential surveillance. Then they remotely intercept a drone's radio signals to look for that pattern in the streaming video the drone sends back to its operator. If they spot it, they can determine that the drone is looking at their subject.

In their first demonstration, researchers show how an invasion of privacy against a house can be detected. They use smart film placed on a window and enter a few software commands on a laptop to access the encrypted video the drone operator sees, called the FPV channel. This enables 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.

THE BGU researchers used a "smart film" in the tests to toggle the opacity of several panes of a house's windows. They used a DJI Mavic quadcopter to spy on the house. They demonstrated that the technique was able to detect the changing of the panes from opaque to transparent and back again. Then they used a parabolic antenna and a laptop to intercept the drone's radio signals sent back to the operator, and search the pattern in the encrypted data stream to detect whether the UAV was used for aerial surveillance of the house.

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.

"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," said Ben Nassi, a doctoral student of Prof. Yuval Elovici in BGU's Department of Software and Information Systems Engineering, and a researcher at the BGU Cyber Security Research Center.

Elovici, the center's director as well as the director of Telekom Innovation Labs at BGU, explains, "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."

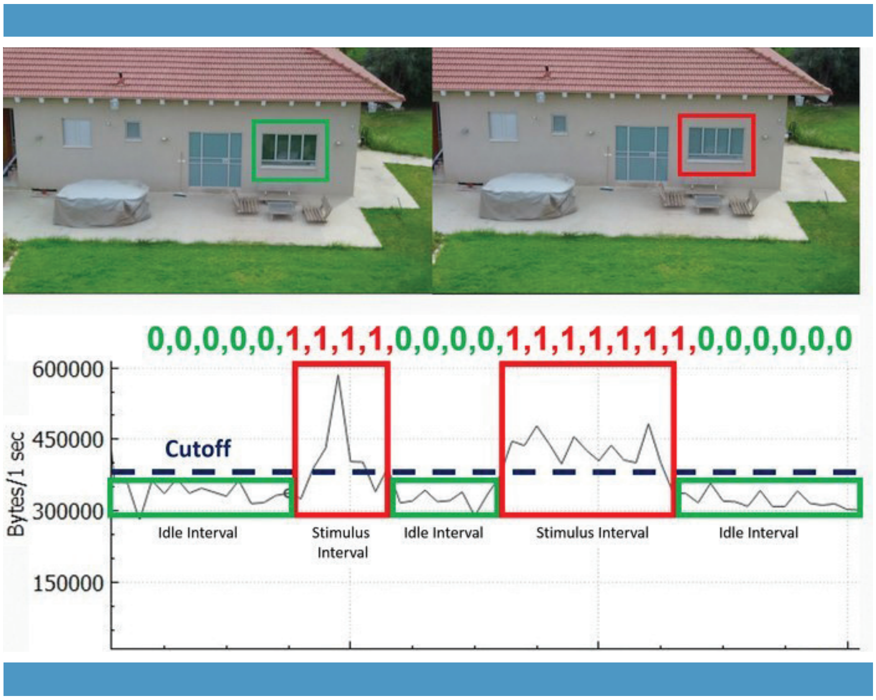
Nassi emphasized that this research shatters the commonly held belief that using encryption to secure the FPV channel prevents someone from knowing he is being tracked. "The secret behind our method is to force controlled physical changes to the captured target that influence the bitrate (data) transmitted on the FPV channel."

"Based on our observations, we demonstrate how an interceptor can perform a side-channel attack to detect whether a target is being streamed by analyzing the encrypted FPV channel that is transmitted from a real drone (DJI Mavic) in two use cases: when the target is a private house and when the target is a subject," noted Nassi.

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

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

Nassi confirmed that their technique works at ranges where it's very difficult to spot a surveillance drone in the sky; the



NASSI ET AL

By changing the opacity of 'smart film' material over a target house's window panes, the researchers can produce a recognizable pattern in the encrypted video communications of a drone watching that house

researchers tested their technique from a range of about 150 feet. The range is scalable by using a more powerful antenna.

Elovici reviewed the system with *The Jerusalem Report* and explained the reason for its development.

"We were concerned about the fact that a person is allowed to fly a drone above private property. It happened in my village where a drone was flying above a neighbor's property. The main issue is that today the drones are so small and their cameras are of such high quality that they can fly above a property and literally invade your privacy by pointing the camera toward you," he said.

He said that "we are lucky" that the drone is transmitting the data encrypted to its operator as this data is public. The data can be observed and cannot be encrypted, but it can be tested.

"What they developed is a mechanism that allows the adding of a covert channel to the communication between the drone and its operator, which is the physical stimulus that was done on the window in the demonstration, and if traces of the physical stimulus are seen in the communication, it is clear that the drone is observing the target and that the drone has invaded the privacy of that person," Elovici said.

In his opinion, the main advantage of this method is that without compromising the operator's privacy, it can be proven that he invaded the other party's privacy. Even if the drone is not visible the physical stimulus will immediately indicate that there is a drone in the area. "Our method can even tell us that there is a drone that is observing us," said Elovici.

He emphasized that drones are a huge security risk, and gave industrial espionage as an example. Today drones are being used for delivery, resulting in an enormous number of drones in the sky, multiplying the risk of being photographed from a drone as almost every drone has a camera.

While most people don't yet equate drones with security risks, they pose an array of threats. Implications for the security industry include sensitive locations (clients' residences, private properties, offices, stadiums, public venues, etc.) can be scouted by drones and intelligence can be gathered, which could reveal weaknesses in the security arrangement and leave a site vulnerable to attack.

In response to the question of what the impact of the research is, the research team said this is a game changer in the battle on privacy: It empowers the victim.

"While many methods have been suggested in recent years to detect the presence of a nearby drone, this research is the first to introduce methods that distinguish between the legitimate and illegitimate (for purposes of privacy invasion) use of a nearby drone. These days, consumer drones are used to conduct privacy invasion attacks throughout the world, however, no tool currently exists for showing that a specific drone is being used to stream a target," concluded the research team.

The research team included Raz Ben-Netanel, a student in BGU's Department of Communication Systems Engineering, and Prof. Adi Shamir from the Weizmann Institute of Science who conceived the technique.

In the published paper which details this process more thoroughly, Ben Nassi explained that this method is not only absolutely functional at determining whether a UAV is looking at you or your property or not, but that it's the first of its kind.

"This is the first method to tell what is being captured in a drone's channel. You can observe without any doubt that someone is watching," he said. "If you can control the stimulus and intercept the traffic as well, you can fully understand whether a specific object is being streamed." ■