Security vulnerabilities detected in drones made by DJI

March 2 2023, by Julia Weiler

The security of drones was already the subject of Nico Schiller's master's thesis at Ruhr University Bochum. He is currently researching this topic for his doctorate. Credit: RUB, Marquard

Researchers from Bochum and Saarbrücken have detected security

vulnerabilities, some of them serious, in several drones made by the manufacturer DJI. These enable users, for example, to change a drone's serial number or override the mechanisms that allow security authorities to track the drones and their pilots. In special attack scenarios, the drones can even be brought down remotely in flight.

The team headed by Nico Schiller of the Horst Görtz Institute for IT Security at Ruhr University Bochum, Germany, and Professor Thorsten Holz, formerly in Bochum, now at the CISPA Helmholtz Center for Information Security in Saarbrücken, will present their findings at the Network and Distributed System Security Symposium (NDSS). The conference will take place from February 27 to March 3 in San Diego, USA.

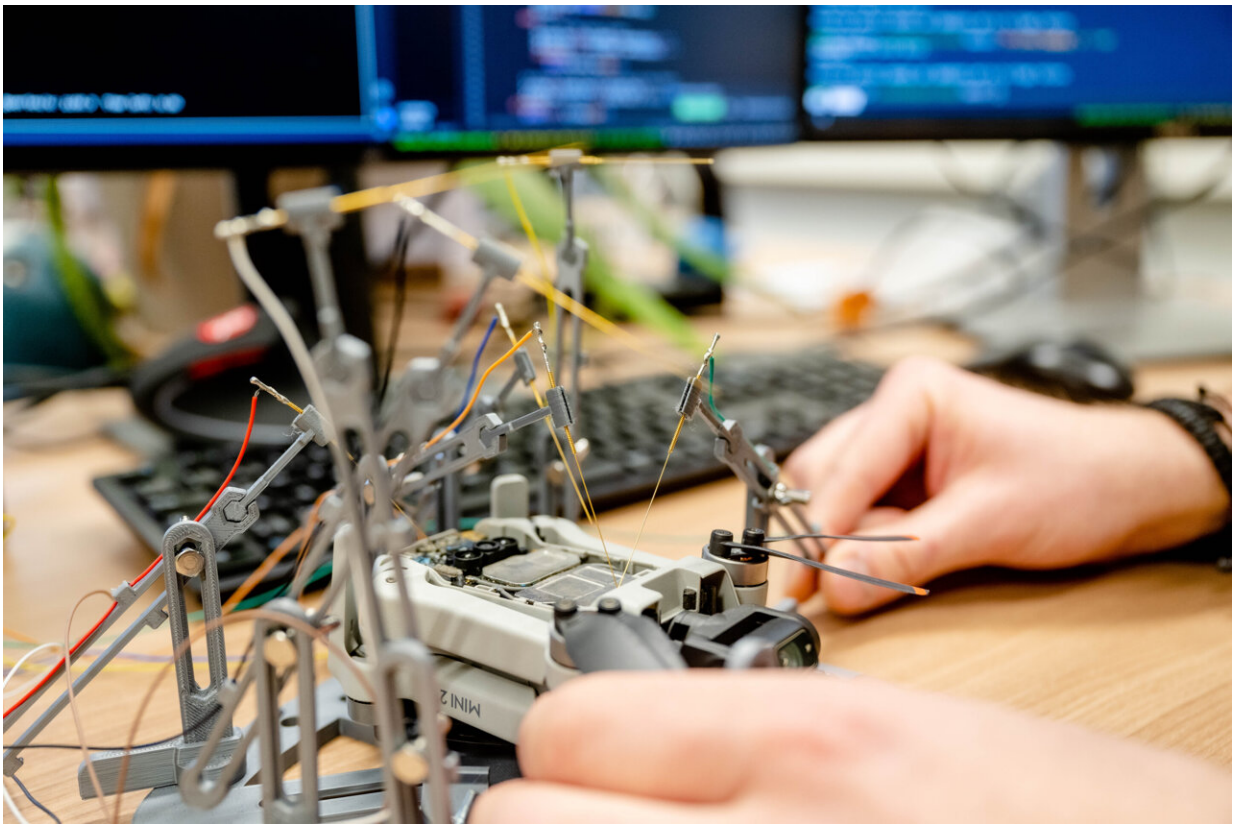
The researchers informed DJI of the 16 detected vulnerabilities prior to releasing the information to the public; the manufacturer has taken steps towards fixing them.

Four models put to the test

The team tested three DJI drones of different categories: the small DJI Mini 2, the medium-sized Air 2, and the large Mavic 2. Later, the IT experts reproduced the results for the newer Mavic 3 model as well. They fed the drones' hardware and firmware a large number of random inputs and checked which ones caused the drones to crash or made unwanted changes to the drone data such as the serial number—a method known as fuzzing. To this end, they first had to develop a new algorithm.

"We often have the entire firmware of a device available for the purpose of fuzzing. Here, however, this was not the case," says Nico Schiller. Because DJI drones are relatively complex devices, the fuzzing had to be performed in the live system. "After connecting the drone to a laptop,

we first looked at how we could communicate with it and which interfaces were available to us for this purpose," says the researcher from Bochum. It turned out that most of the communication is done via the same protocol, called DUML, which sends commands to the drone in packets.



The researchers looked for security gaps in the firmware and scrutinized the inner workings of the drones. Credit: RUB, Marquard

Four severe errors

The fuzzer developed by the research group thus generated DUML data packets, sent them to the drone and evaluated which inputs caused the

drone's software to crash. Such a crash indicates an error in the programming. "However, not all security gaps resulted in a crash," says Thorsten Holz. "Some errors led to changes in data such as the serial number."

To detect such logical vulnerabilities, the team paired the drone with a mobile phone running the DJI app. They could thus periodically check the app to see if fuzzing was changing the state of the drone.

All of the four tested models were found to have security vulnerabilities. In total, the researchers documented 16 vulnerabilities. The DJI Mini 2, Mavic Air 2 and Mavic 3 models had four serious flaws. For one, these bugs allowed an attacker to gain extended access rights in the system.

"An attacker can thus change log data or the serial number and disguise their identity," explains Thorsten Holz. "Plus, while DJI does take precautions to prevent drones from flying over airports or other restricted areas such as prisons, these mechanisms could also be overridden." Furthermore, the group was able to crash the flying drones mid-air.

In future studies, the Bochum-Saarbrücken team intends to test the security of other drone models as well.

Location data is transmitted unencrypted

In addition, the researchers examined the protocol used by DJI drones to transmit the location of the drone and its pilot so that authorized bodies—such as security authorities or operators of critical infrastructure—can access it.

By reverse engineering DJI's firmware and the radio signals emitted by the drones, the research team was able to document the tracking protocol

called "DroneID" for the first time. "We showed that the transmitted data is not encrypted, and that practically anyone can read the location of the pilot and the drone with relatively simple methods," concludes Nico Schiller.

More information: Paper: www.ndss-symposium.org/ndss-pa … ase-of-djis-droneid/

Conference: www.ndss-symposium.org/

Provided by Ruhr-Universitaet-Bochum