Researcher demonstrates how easy it is to hack police-type drone

March 3 2016, by Bob Yirka

IBM researcher Nils Rodday has given a presentation at this year's RSA

Security Conference demonstrating how easy it is to hack an unknown brand of police drone. He reported that he discovered the technique while still a graduate student at the University of Twente in the Netherlands.

Drones have, of course, become more and more commonplace as the technology improves and prices fall, and while some have become inexpensive enough for consumers to purchase as a hobby, others offer more features and still run into the tens of thousands of dollars; one application of the more expensive drone is use by police departments to help search areas very quickly. But now, according to Rodday, such drones may be at risk of not only being hacked, but of being taken over completely while in flight by someone equipped with nothing more than an inexpensive radio device and a laptop.

The problem, Rodday explained, is that communications between such drones and their pilot are not properly encrypted—because adding encryption tends to introduce delays in response by the drone, which of course impedes performance. More specifically, he pointed out that drones make use of wired-equivalent privacy encryption between the telemetry module and the tablet computer the user holds to control the drone, which is widely known to be easy to crack. Thus, anyone within WiFi range could break into the module and send false commands to the drone. That is just the first problem, the second is that the technology that exists to allow communications between the telemetry module and the drone, is based on Xbee chips, which have built in encryption—but in drones, that encryption is disabled to enhance responsiveness. The result Rodday reports, is a situation where a person with a simple radio device connected to a laptop can send disruption signals to a drone system that causes the signals from the original pilot to be ignored, as the new hacker-pilot takes over complete control.

Rodday also divulged that he has been pressured to release the name of

the company that makes the type of drone he hacked, but has refused, pointing out that the problem is not with just a single make, model or manufacturer, it is with drones in general. He believes more work needs to be done to prevent such easy hacking moving forward.