

28.07.2011. Forbes

Flying Drone Can Crack Wi-Fi Networks, Snoop On Cell Phones

How do one ex-Air Force official and one former airplane hobby shop owner, both of whom happen to have decades of experience as network security contractors for the military, spend their weekends? Building a flying, unmanned, automated password-cracking, Wi-Fi-sniffing, cell-phone eavesdropping spy drone, of course.

At the Black Hat and Defcon security conferences in Las Vegas next week, Mike Tassej and Richard Perkins plan to show the crowd of hackers a year's worth of progress on their Wireless Aerial Surveillance Platform, or WASP, the second year Tassej and Perkins have displayed the 14-pound, six-foot long, six-foot wingspan unmanned aerial vehicle. The WASP, built from a retired Army target drone converted from a gasoline engine to electric batteries, is equipped with an HD camera, a cigarette-pack sized on-board Linux computer packed with network-hacking tools including the BackTrack testing toolset and a custom-built 340 million word dictionary for brute-force guessing of passwords, and eleven antennae.

"This is like Black Hat's greatest hits," Tassej says. "And it flies."

On top of cracking wifi networks, the upgraded WASP now also performs a new trick: impersonating the GSM cell phone towers used by AT&T and T-Mobile to trick phones into connecting to the plane's antenna rather than their carrier, allowing the drone to record conversations and text messages on a 32 gigabytes of storage. A 4G T-mobile card routes the communications through voice-over-Internet or traditional phone connections to avoid dropping the call. "Ideally, the target won't even know he's being spied on," says Tassej.

That GSM hack is based on a demonstration that security researcher Chris Paget performed at Defcon last year, showing that with a powerful enough antenna placed close enough to target phones, the victims' handsets can be tricked into connecting to Paget's setup instead of the carrier's tower. Perkins and Tassej have implemented the same tools in their airborne hacking machine, and like Paget, used a portion of the radio frequency band set aside for Ham radios to avoid violating FCC regulations. They don't plan to demonstrate the phone-hacking trick at the conference, and tested it only in isolated conditions to ensure their flying contraption wasn't illegally eavesdropping on random strangers' phones. "We want to make sure we're not stepping on any cell providers' toes," says Tassej.

And why build a digital spy drone? Perkins, an Air Force contractor focused on cybersecurity who once owned a airplane hobby shop, and Tassej, an ex-Air Force consultant with Engineering Systems Solutions, say they wanted to demonstrate the vulnerability of government and corporate facilities to a nimble eavesdropping machine that can cover large distances and circle above a target. Though it requires remote control

to take off and land, WASP can be set to fly a pre-programmed course once airborne and loiter around any chosen area. "We wanted to bring to light how far the consumer industry has progressed, to the point where public has access to technologies that put companies, and even governments at risk from this new threat vector that they're not aware of," says Perkins.

A military base like Area 51, Tassej points out, is surrounded by more than 25 miles of empty land to obscure it from outside snoops. "With WASP, we can cover that distance in about 20 minutes," he says. "With radar designed specifically *not* to see birds, it's very difficult to protect yourself from an object coming out of the sky and flying low."

WASP's design, complete with two eyes and a black-and-yellow striped paint job, isn't not exactly designed for stealth. But aside from showing real-world security risks, Tassej and Perkins also shared a goal just as appealing to Black Hat and Defcon's crowd: pulling off a fantastically elaborate hack. "The number one reason we did this was because we were told it wouldn't be possible," says Perkins. "Neither of us like hearing that."

<http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/>