Hacked satellite systems could launch microwave-like attacks, expert warns

amp.theguardian.com/technology/news-blog/2018/aug/09/satellite-system-hacking-attacks-ships-planes-military

Alex Hern August 9, 2018

The satellite communications that ships, planes and the military use to connect to the internet are vulnerable to hackers that, in the worst-case scenario, could carry out “cyber-physical attacks”, turning satellite antennas into weapons that operate, essentially, like microwave ovens.

According to research presented at the Black Hat information security conference in Las Vegas, a number of popular satellite communication systems are vulnerable to the attacks, which could also leak information and hack connected devices. The attacks, which are merely a nuisance for the aviation sector, could pose a safety risk for military and maritime users, the research claims.

Ruben Santamarta, a researcher for the information security firm IOActive, carried out the study, building on research he presented in 2014. “The consequences of these vulnerabilities are shocking,” Santamarta said. “Essentially, the theoretical cases I developed four years ago are no longer theoretical.”

The attack works by connecting to the satellite antenna from the ground, through the internet, and then using security weaknesses in the software that operates the antenna to seize control.

From there, the potential damage varies. At the very least, the attack offers the ability to disrupt, intercept or modify all communications passed through the antenna, allowing an attacker to, for instance, eavesdrop on emails sent through an in-flight wifi system, or

attempt to launch further hacking attacks against devices connected to the satellite network.

And in some situations, the safety risk is higher still. In the case of the military, for instance, the attack also exposes the location of the satellite antenna, since they usually need an attached GPS device to function. “If you can pinpoint the location of a military base, that’s a safety risk,” Santamarta noted, “but not for a plane or a ship”, whose locations are generally public.

Both military and maritime users are also at the risk of what Santamarta described as “cyber-physical attacks”: repositioning the antenna and setting its output as high as it will go, to launch a “high intensity radio frequency (HIRF) attack”.

“We’re basically turning Satcom devices into radio frequency weapons,” Santamarta said. “It’s pretty much the same principle behind the microwave oven.” Even if the antenna can’t be used to physically injure soldiers, passengers or crew, a HIRF attack can also cause physical damage to electrical systems.

The safety risk is not as high for the aviation sector, Santamarta said, because planes tend to be built with a significant amount of HIRF shielding in place. “The industry has done a good job of putting strong design and testing standards in place that would protect critical flight systems from HIRF attacks using airborne Satcom equipment,” Santamarta writes in his report, adding that it “should be commended for identifying an emerging threat”.

Following the research, IOActive worked with the aviation industry to ensure that affected airlines are no longer exposing their fleets, and passengers, to the open internet. But while the company reported the issues with the maritime and military uses of satellite technology to US and EU regulators, it has not received any further information about fixes.