Researchers successfully spoof an $80 million yacht at sea (w/ Video)

July 31 2013

This summer, a radio navigation research team from The University of Texas at Austin set out to discover whether they could subtly coerce a 213-foot yacht off its course, using a custom-made GPS device.

Led by assistant professor Todd Humphreys of the Department of Aerospace Engineering and Engineering Mechanics at the Cockrell School of Engineering, the team was able to successfully spoof an $80 million private yacht using the world's first openly acknowledged GPS spoofing device. Spoofing is a technique that creates false civil GPS

signals to gain control of a vessel's GPS receivers. The purpose of the experiment was to measure the difficulty of carrying out a spoofing attack at sea and to determine how easily sensors in the ship's command room could identify the threat.

The researchers hope their demonstration will shed light on the perils of navigation attacks, serving as evidence that spoofing is a serious threat to marine vessels and other forms of transportation. Last year, Humphreys and a group of students led the first public capture of a GPS-guided unmanned aerial vehicle (UAV), or drone, using a GPS device created by Humphreys and his students.

"With 90 percent of the world's freight moving across the seas and a great deal of the world's human transportation going across the skies, we have to gain a better understanding of the broader implications of GPS spoofing," Humphreys said. "I didn't know, until we performed this experiment, just how possible it is to spoof a marine vessel and how difficult it is to detect this attack."

In June, the team was invited aboard the yacht, called the White Rose of Drachs, while it traveled from Monaco to Rhodes, Greece, on the Mediterranean Sea. The experiment took place about 30 miles off the coast of Italy as the yacht sailed in international waters.

From the White Rose's upper deck, graduate students Jahshan Bhatti and Ken Pesyna broadcasted a faint ensemble of civil GPS signals from their spoofing device—a blue box about the size of a briefcase—toward the ship's two GPS antennas. The team's counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship's navigation system.

Unlike GPS signal blocking or jamming, spoofing triggers no alarms on the ship's navigation equipment. To the ship's GPS devices, the team's

false signals were indistinguishable from authentic signals, allowing the spoofing attack to happen covertly.

Once control of the ship's navigation system was gained, the team's strategy was to coerce the ship onto a new course using subtle maneuvers that positioned the yacht a few degrees off its original course. Once a location discrepancy was reported by the ship's navigation system, the crew initiated a course correction. In reality, each course correction was setting the ship slightly off its course line. Inside the yacht's command room, an electronic chart showed its progress along a fixed line, but in its wake there was a pronounced curve showing that the ship had turned.

"The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line," Humphreys said.

After several such maneuvers, the yacht had been tricked onto a parallel track hundreds of meters from its intended one—the team had successfully spoofed the ship.

The experiment helps illustrate the wide gap between the capabilities of spoofing devices and what the transportation industry's technology can detect, Humphreys said.

Chandra Bhat, director of the Center for Transportation Research at The University of Texas at Austin, believes that the experiment highlights the vulnerability of the transportation sector to such attacks.

"The surprising ease with which Todd and his team were able to control a (multimillion) dollar yacht is evidence that we must invest much more in securing our transportation systems against potential spoofing," Bhat said.

It's important for the public and policymakers to understand that

spoofing poses a threat that has far-reaching implications for transportation, Humphreys said.

"This experiment is applicable to other semi-autonomous vehicles, such as aircraft, which are now operated, in part, by autopilot systems," Humphreys said. "We've got to put on our thinking caps and see what we can do to solve this threat quickly."

Provided by University of Texas at Austin