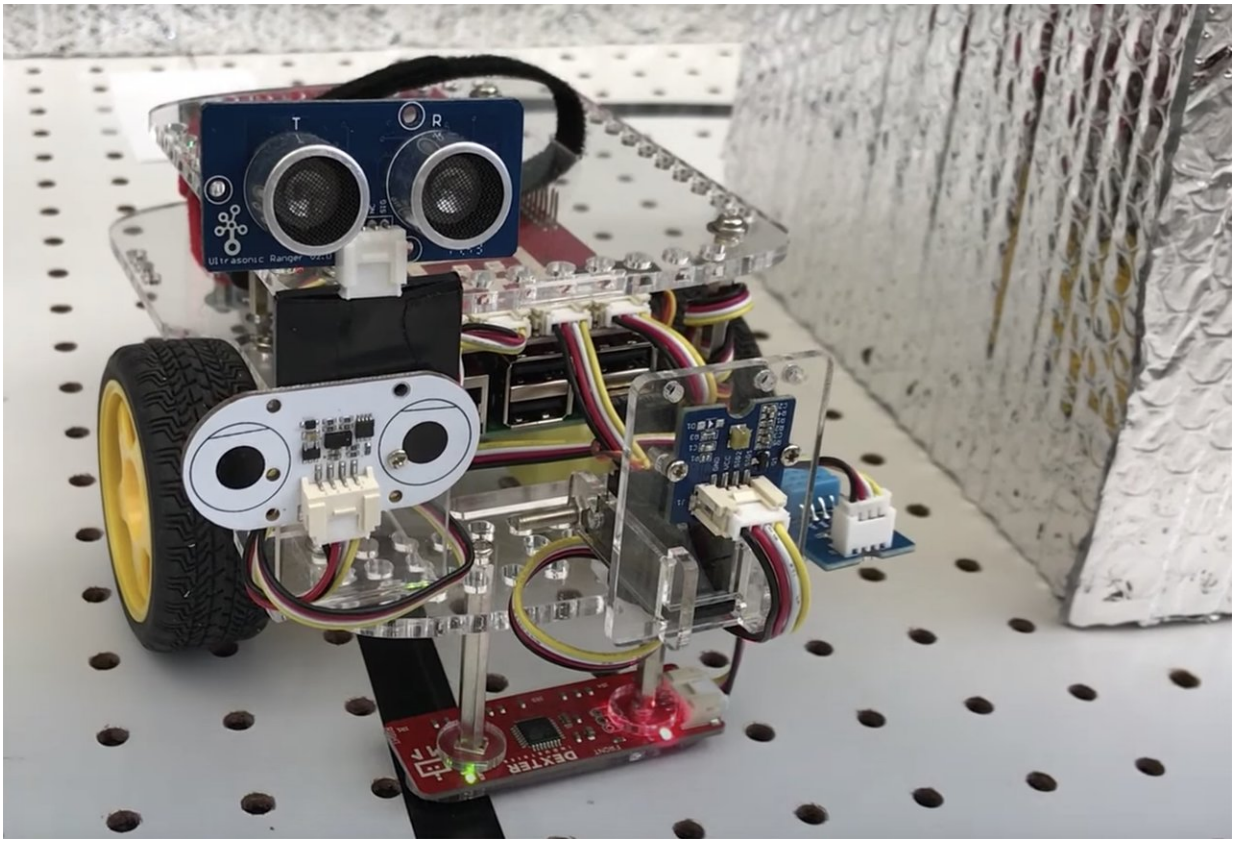
Robot designed to defend factories against cyberthreats

April 3 2018, by Josh Brown



Credit: Georgia Institute of Technology

It's small enough to fit inside a shoebox, yet this robot on four wheels has a big mission: keeping factories and other large facilities safe from hackers.

Meet the HoneyBot.

Developed by a team of researchers at the Georgia Institute of Technology, the diminutive device is designed to lure in digital troublemakers who have set their sights on industrial facilities. HoneyBot will then trick the bad actors into giving up valuable information to cybersecurity professionals.

The decoy robot arrives as more and more devices – never designed to operate on the Internet – are coming online in homes and factories alike, opening up a new range of possibilities for hackers looking to wreak havoc in both the digital and physical world.

"Robots do more now than they ever have, and some companies are moving forward with, not just the assembly line robots, but free-standing robots that can actually drive around factory floors," said Raheem Beyah, the Motorola Foundation Professor and interim Steve W. Chaddick School Chair in Georgia Tech's School of Electrical and Computer Engineering. "In that type of setting, you can imagine how dangerous this could be if a hacker gains access to those machines. At a minimum, they could cause harm to whatever products are being produced. If it's a large enough robot, it could destroy parts or the assembly line. In a worst-case scenario, it could injure or cause death to the humans in the vicinity."

Internet security professionals long have employed decoy computer systems known as "honeypots" as a way to throw cyberattackers off the trail. The research team applied the same concept to the HoneyBot, which is partially funded with a grant from the National Science Foundation. Once hackers gain access to the decoy, they leave behind valuable information that can help companies further secure their networks.

"A lot of cyberattacks go unanswered or unpunished because there's this level of anonymity afforded to malicious actors on the internet, and it's hard for companies to say who is responsible," said Celine Irvene, a Georgia Tech graduate student who worked with Beyah to devise the new robot. "Honeypots give security professionals the ability to study the attackers, determine what methods they are using, and figure out where they are or potentially even who they are."

The gadget can be monitored and controlled through the internet. But unlike other remote-controlled robots, the HoneyBot's special ability is tricking its operators into thinking it is performing one task, when in reality it's doing something completely different.

"The idea behind a honeypot is that you don't want the attackers to know they're in a honeypot," Beyah said. "If the attacker is smart and is looking out for the potential of a honeypot, maybe they'd look at different sensors on the robot, like an accelerometer or speedometer, to verify the robot is doing what it had been instructed. That's where we would be spoofing that information as well. The hacker would see from looking at the sensors that acceleration occurred from point A to point B."

In a factory setting, such a HoneyBot robot could sit motionless in a corner, springing to life when a hacker gains access – a visual indicator that a malicious actor is targeting the facility.

Rather than allowing the hacker to then run amok in the physical world, the robot could be designed to follow certain commands deemed harmless – such as meandering slowly about or picking up objects – but stopping short of actually doing anything dangerous.

So far, their technique seems to be working.

In experiments designed to test how convincing the false sensor data would be to individuals remotely controlling the device, volunteers in December 2017 used a virtual interface to control the robot and could not to see what was happening in real life. To entice the volunteers to break the rules, at specific spots within the maze, they encountered forbidden "shortcuts" that would allow them to finish the maze faster.

In the real maze back in the lab, no shortcut existed, and if the participants opted to go through it, the robot instead remained still. Meanwhile, the volunteers – who have now unwittingly become hackers for the purposes of the experiment – were fed simulated sensor data indicating they passed through the shortcut and continued along.

"We wanted to make sure they felt that this robot was doing this real thing," Beyah said.

In surveys after the experiment, participants who actually controlled the device the whole time and those who were being fed simulated data about the fake shortcut both indicated that the data was believable at similar rates.

"This is a good sign because it indicates that we're on the right track," Irvene said.

Provided by Georgia Institute of Technology