Securing the food pipeline from cyberattacks

October 11 2023, by Jes Hernandez

The Food and Agriculture Risk Modeling project, led by Pacific Northwest National Laboratory, is investigating the cybersecurity vulnerabilities, risks, and consequences of smart technology to secure the food pipeline. Credit: Shannon Colson | Pacific Northwest National Laboratory

Sensors detecting the amount of food that herds of cattle are eating. Machines taking thousands of photos of fruit per second to detect their defects and sort them by quality. Robots packing fruit and vegetables into bags and boxes for purchase at grocery stores.

The future of farming is advanced technology, and already there are many examples of technologies controlled by smart devices and computer systems. They have created opportunity for larger economic yields and promise safer, more efficient, and environmentally friendly processes.

But has the same technology designed to improve agriculture and food production created potential risk for cyberattacks?

"Food and agriculture are critical sectors of our economy and livelihood. If it's compromised, the ramifications could be immense," said Mary Lancaster, Pacific Northwest National Laboratory (PNNL) epidemiologist and data scientist.

The Food and Agriculture Risk Modeling (FARM) project, led by Lancaster and researchers at PNNL, is the first investigation into cybersecurity vulnerabilities of an increasingly smart food and agriculture sector for the Department of Homeland Security.

"This is a first attempt at trying to characterize how big and where those vulnerabilities are, and the impacts if something goes wrong," said Lancaster.

From farm to table and all the smart technology in between Cyberattacks have already caused economic issues for businesses in the food and agriculture sector. In 2021, a meat processing company experienced a ransomware attack that affected its global operations and led the company to pay $11 million in ransom.

Despite the challenges, technology in agriculture is still rapidly developing—spurring what some are calling the "fourth agriculture revolution."

"I think there are assumptions that agriculture is primarily small mom and pop farms without a lot of technology," said Lancaster. "The profit margins in agriculture are so small that adopting technology increases efficiency and gleans every last bit of income from crops and livestock, helping farmers compete and succeed."

Technology can extend the life of seasonal produce, ensuring that people around the world have access to fruits and vegetables up to one year after harvest. For example, apples are typically harvested from the end of July until mid-November, but certain types of apples can be purchased at markets all year round and taste as if they were just picked from a tree.

How? Controlled-atmosphere technology uses a scientific process to make apples artificially hibernate by adjusting the temperature and gases of the atmosphere in a sealed-tight room monitored by sensors. Refrigeration technicians reduce oxygen to an extremely low percentage and carefully regulate temperature, humidity, nitrogen, and carbon dioxide. The controlled atmosphere slows down the breathing of apples and, in effect, slows the ripening process.

Calculating the consequences

While the future of farming continues to be defined, FARM is proactively identifying the potential vulnerabilities within smart technology systems and calculating the consequences of successful cyberattacks to the economy, animals, humans, and the environment—from financial losses to contamination of food and even death.

"We're looking at all 'what if' scenarios at multiple scales, including compromised equipment, supply chain issues, or even what could happen if manufacturing databases were altered to no longer meet specifications and ingredient levels," said Lancaster. "For example, if eggs were included in something that shouldn't have eggs, what are the impacts to people with food allergies or the manufacturer?"

A cyberattack to a controlled atmosphere room could compromise a year's worth of fresh apple supply—or worse, cause harm to people loading or unloading the rooms.

A sample scenario in the FARM framework describes the impact of cyberattacks on animals. In the scenario, the cyberattack prevents a small, non-invasive sensor patch from reporting data points like heart function and respiration rate of cattle back to farmers, allowing the presence of sick animals in the herd to remain hidden. FARM calculates the number of cattle exposed and the likeliness of disease transmission to other animals. The consequences include death of animals, costly veterinary treatment, quarantine, and decontamination of the farm premises.

"After COVID, the world started paying more attention to how animals, plants, and human health are related," said Lauren Charles, FARM project manager and veterinarian. "The project uses a One Health approach, aiming to secure the health of agricultural animals and crop plants, which directly impacts the health of humans and their shared environments."

Researchers centered in an agricultural community

PNNL—located in the Tri-Cities region of Washington—is surrounded by farms and food processing centers in a rich agriculture basin. It's an ideal location for the multi-disciplinary FARM team, which includes data scientists, cybersecurity experts, and researchers with agriculture and food backgrounds.

"Being in an ag center helps provide local examples for the project. Many people on our team grew up in agriculture," said Lancaster. "One person became interested in this work because he saw cybersecurity vulnerabilities on his own family farm, specifically in irrigation."

Lancaster's grandparents were farmers. Her connection to agriculture builds passion for this work, but more so, she said, "I've always been interested in modeling and figuring out how systems work. My background is in biosecurity and cybersecurity, and this research is an intersection of those two—it is cybersecurity meets agriculture."

The team is partnering with farms in the region to understand more about the technology being used and the risks associated with that technology. The FARM models will continue to be developed into the next year.

"We are thinking about this work holistically because of its wide impact. Cyberattacks will not only affect the environment and livestock, but can cause harm to humans too," said Lancaster. "This is a huge problem space that no one else is addressing, but we're making progress."

Provided by Pacific Northwest National Laboratory