Medical Xpress

Five ways to keep vaccine cold storage equipment safe from hackers

October 20 2021

Low-temperature freezers like this one at University of Michigan Hospital in Ann Arbor, are used to keep vaccines and other medicines super-cold. Credit: Joe Hallisy, Michigan Medicine

Electronics in the "cold chain" that health systems use to keep items like COVID-19 vaccines ultra-cold during storage and transport are surprisingly vulnerable to hacking, but there are ways that health systems

can protect themselves.

A University of Michigan study commissioned by a major health system found that an attacker located near equipment like freezers and coolers could use electromagnetic interference generated by simple devices like walkie-talkies to fool temperature sensors into giving false readings.

The interference could cause a cooler's temperature monitor to falsely indicate that the vaccine inside has become too warm to use, or it could cause a freezer to malfunction and spoil its contents.

The good news is there are simple steps that hospitals and health systems can take to protect themselves. U-M electrical engineering and computer science associate professor Kevin Fu led the study as part of his post at U-M. Fu later joined the FDA as acting director of medical device cybersecurity. He recommends the following five steps:

Restrict access to data like temperature displays

A prospective attacker might try to devise a hack using trial and error—trying several different types of electromagnetic interference (EMI), such as radio waves from walkie-talkies, while watching temperature displays or other data to see which type of interference is effective.

Health systems can protect against this kind of attacker by making data points like temperature readouts less visible. This could be done by:

- Installing blinders on temperature displays, similar to those on ATMs and voting machines.
- Eliminating real-time temperature displays when possible.
- Moving displays to make them less visible—for example, turning a display so it can't be seen through a room's doorway.

- Restricting access to areas where temperature displays are located.

Keep the details about your sensors confidential

If a prospective attacker knows which sensors you use, they could buy an identical model, then work out the details of an attack off-site. Health systems can reduce the likelihood of this by keeping model numbers and other details about the temperature sensors in equipment like coolers and freezers confidential.

Keep the locations of your sensors confidential, and move them frequently

To successfully carry out an attack, a hacker must put an EMI device within a certain distance of the equipment to be hacked. There are a number of ways that health systems can make that more difficult. They include:

- Keeping the locations of cold chain equipment confidential.
- Frequently moving equipment to different locations.
- Moving equipment toward the center of the rooms where they're stored. This makes it more difficult to carry out an attack from an adjoining room.

Select the lowest possible sensor sampling rate

Temperature sensors take measurements at pre-set sampling rates—for example, once every five minutes. And a sensor with a lower sampling rate provides less data that a hacker could use to carry out an attack.

With this in mind, it makes sense to select a sensor with the lowest

sampling rate necessary for keeping vaccines and other ultra-cold items safe. Some sensors have adjustable sampling rates, and it's smart to adjust them to the lowest sampling rate necessary for keeping items safe.

Use a sensor that's less susceptible to electromagnetic energy

Depending on specific application, it may be possible to use a sensor that's less susceptible to interference than a traditional thermocouple, like an on-chip integrated temperature sensor or a chemical-based temperature indicator.

However, most of these types of sensors can't operate at temperatures below -40 degrees Celsius, so it's critical to carefully match sensors to specific applications.

More information: Yan Long et al, Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats, *Biomedical Instrumentation & Technology* (2021). DOI: 10.2345/0890-8205-55.3.112

Provided by University of Michigan