Cyber vulnerability discovered in networks used by spacecraft, aircraft and energy generation systems

November 15 2022, by Zach Champion

Credit: Pixabay/CC0 Public Domain

A major vulnerability in a networking technology widely used in critical infrastructures such as spacecraft, aircraft, energy generation systems and industrial control systems was exposed by researchers at the

University of Michigan and NASA.

It goes after a network protocol and hardware system called time-triggered ethernet, or TTE, which greatly reduces costs in high-risk settings by allowing mission-critical devices (like flight controls and life support systems) and less important devices (like passenger WiFi or data collection) to coexist on the same network hardware. This blend of devices on a single network arose as part of a push by many industries to reduce network costs and boost efficiency.

That coexistence has been considered safe for more than a decade, predicated on a design that prevented the two types of network traffic from interfering with one another. The team's attack, called PCspooF, was the first of its kind to break this isolation.

In one compelling demonstration, the team used real NASA hardware to recreate a planned Asteroid Redirection Test. The experimental setup controlled a simulated crewed capsule, specifically at the point in the mission when the capsule prepared to dock with a robotic spacecraft.

"We wanted to determine what the impact would be in a real system," said Baris Kasikci, the Morris Wellman Faculty Development Assistant Professor of Computer Science and Engineering. "If someone executed this attack in a real spaceflight mission, what would the damage be?"

With one small malicious device, the team was able to seamlessly introduce disruptive messages to the system, creating a cascading effect that ended in the capsule veering off course and missing its dock entirely.

Here's how it works: The attack emulates the network switches, which are high-stakes traffic controllers in TTE networks, by sending out fake synchronization messages. These messages are normally intended to

keep network devices running on a shared schedule, allowing the most important devices to communicate quickly.

"Normally, no device besides a network switch is allowed to send this message, so in order to get the switch to forward our malicious message, we conducted electromagnetic interference into it over an Ethernet cable," said Andrew Loveless, U-M doctoral student in computer science and engineering and subject matter expert at the NASA Johnson Space Center.

That interference serves as an envelope for the fake synchronization message. The noise causes just enough of a gap in the switch's normal operation to allow the message to pass through. An easily concealed bit of circuitry on a malicious device, connected to the network via Ethernet, can inject these messages as many times as necessary to throw everything out of whack.

"Once the attack is underway, the TTE devices will start sporadically losing synchronization and reconnecting repeatedly," Loveless said.

This disruption will gradually lead to time-sensitive messages being dropped or delayed, causing systems to operate unpredictably and, at times, catastrophically. But the researchers explain how to prevent this attack, too.

Replacing copper Ethernet with fiber optic cables or installing optical isolators between switches and untrusted devices would eliminate the risk of electromagnetic interference, though this would come with cost and performance tradeoffs. Other options involve changes to the network layout, so that malicious synchronization messages can never access the same path taken by the legitimate ones.

"Some of these mitigations could be implemented very quickly and

cheaply," Kasikci said.

The team disclosed their findings and proposed mitigations to major companies and organizations using TTE and to device manufacturers in 2021, and the study is to be published as part of the *2023 IEEE Symposium on Security and Privacy (SP)*.

"Everyone has been highly receptive about adopting mitigations," Loveless said. "To our knowledge, there is not a current threat to anyone's safety because of this attack. We have been very encouraged by the response we have seen from industry and government."

More information: Baris Kasikci et al, PCspooF: Compromising the Safety of Time-Triggered Ethernet, *2023 IEEE Symposium on Security and Privacy (SP)* (2022). DOI: 10.1109/SP46215.2023.00033. www.computer.org/csdl/proceedi … 3600a572/1He7YmWugq4

Provided by University of Michigan