Identifying a vulnerability in critical spacecraft networks

January 6 2023

Credit: Pixabay/CC0 Public Domain

When NASA docks two spacecraft in orbit, timing is critical. Their movements must be precisely synchronized with each other to prevent catastrophic failure, which means the computer networks that control their thrusters must not be disrupted for even a split second; instructions on exactly how and when to move must be delivered on time, every time.

Linh Thi Xuan Phan, Associate Professor in Penn Engineering's Department of Computer and Information Science, has collaborated with a team of researchers at the University of Michigan and NASA to identify a critical security flaw in the networking approach used in these and other safety-critical systems.

Known as Time-Triggered Ethernet, or TTE, this approach has been used for more than a decade in aerospace, aviation and heavy industry applications. In those contexts, many different types of information are constantly traveling over their computer networks, but not all require the same level of timing precision. Time-Triggered Ethernet guarantees that the most critical signals get priority, removing the need for separate network hardware dedicated to them.

Having multiple types of signals on the same physical network via TTE is especially important for NASA, which must account for every ounce of weight on a spacecraft. However, the research team was the first to show that TTE's safety guarantees could be compromised via electromagnetic interference, disrupting the timing of the high-priority signals enough to cause critical failure on a simulated docking procedure.

Along with Andrew Loveless, Ronald Dreslinski and Baris Kasikci of the University of Michigan, Phan published these findings in the *Proceedings of the 2023 IEEE Symposium on Security and Privacy*.

While working at NASA's Johnson Space Center, Loveless began investigating the possibility of this security flaw with simulation data. He and his Michigan colleagues recruited Phan, an expert on the safety of cyber-physical systems, to look at a flaw rooted in the hardware of the TTE networks themselves.

They showed that low-priority signals could be sent in such a way that

the Ethernet cables transmitting the message would generate electromagnetic interference, enough to slip a malicious message through switches that would normally block them.

"This approach was in widespread use in critical systems because of the guarantee that the two types of signals could not interfere with each other," says Phan. "But if that assumption is wrong, everything else falls apart."

The team privately disclosed their findings and proposed mitigations—including swapping copper cabling for fiber optics and other optical isolators—to major companies and organizations using TTE and to device manufacturers in 2021.

"Everyone has been highly receptive about adopting mitigations," Loveless says. "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: Andrew Loveless et al, PCspooF: Compromising the Safety of Time-Triggered Ethernet, *Proceedings of the 2023 IEEE Symposium on Security and Privacy* (2023). DOI: 10.1109/SP46215.2023.00033. www.computer.org/csdl/proceedi … 3600a572/1He7YmWugq4

Provided by University of Pennsylvania