SCIENCE & TECHNOLOGY

Identifying a vulnerability in critical spacecraft networks

Penn Engineering's Linh Thi Xuan Phan and a team of researchers have identified a critical security flaw in the networking approach used in aerospace and other safety–critical systems.

When two spacecrafts need to bridge a connection in orbit they dock. This means the onboard computers controlling their thrusters need unfettered communication between one another that cannot be disrupted for even a split second. Instructions on how and when to move must be precisely synchronized and delivered on time, every time.

Penn Engineering's Linh Thi Xuan Phan. (Image: Penn Engineering Today)

Penn engineering's Linh Thi Xuan Phan (https://directory.seas.upenn.edu/linh-thi-xuan-phan/) and collaborators from NASA and the University of Michigan have identified a major security flaw in Time-Triggered Ethernet (TTE), an efficient communication protocol not only used to facilitate spacecraft-to-spacecraft connections but is also widely used in aviation and energy generation.

TTE allows critical systems, like vehicle controls, to share hardware with non-critical systems, like in-flight Wi-Fi, while ensuring they do not interfere with each other. However, their research, published in the *Proceedings of the 2023 IEEE Symposium on Security and Privacy* (https://www.computer.org/csdl/proceedings-article/sp/2023/933600a572/1He7YmWugq4), 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.

The researchers 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. The team reported their findings to several organizations that use TTE, and many are implementing measures to mitigate any potential threats.

"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."

Read more at Penn Engineering Today (https://blog.seas.upenn.edu/identifying-a-vulnerability-in-critical-spacecraft-networks/).

CREDITS	**Evan Lerner** Writer
DATE	**January 5, 2023**
SUBTOPICS	**Computer Science, Research**
SCHOOLS	**School of Engineering & Applied Science**