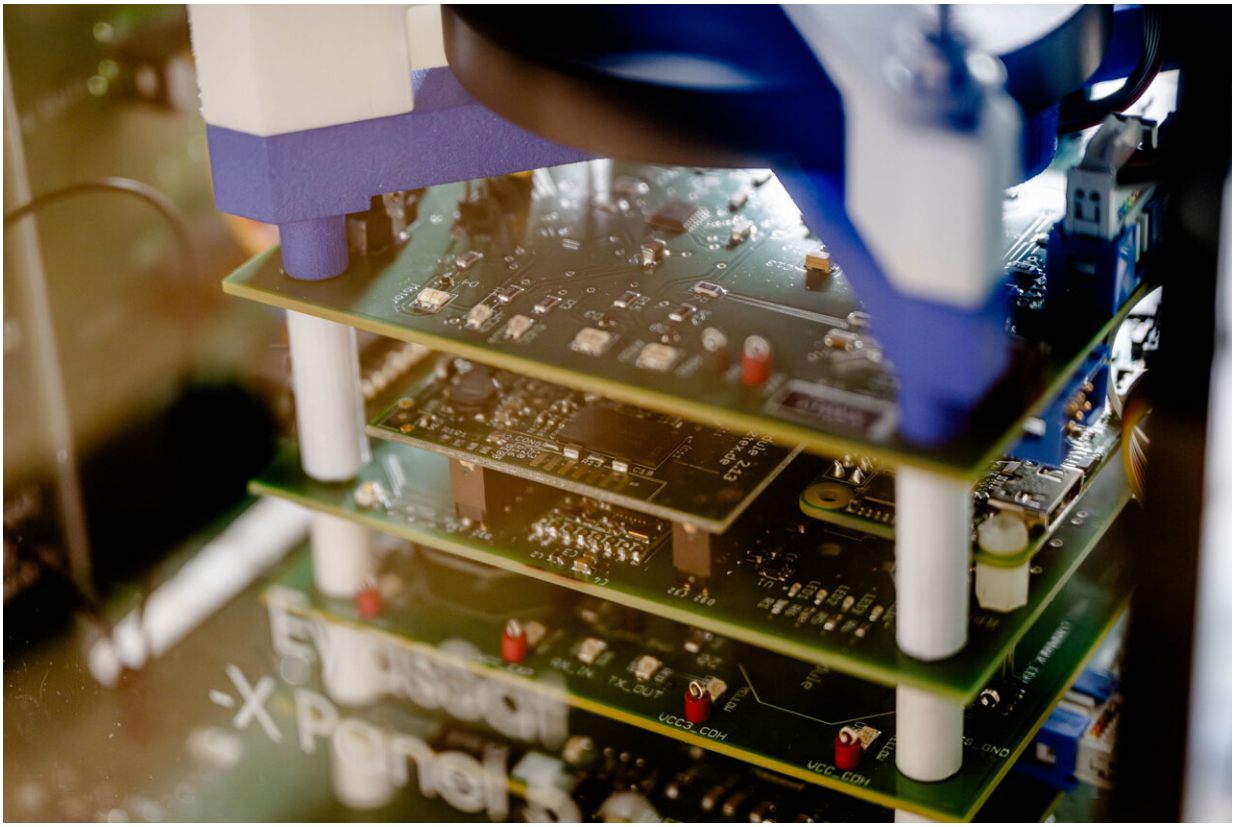
Satellite security lags decades behind the state of the art

July 13 2023, by Julia Weiler



The inside of a small satellite. Credit: RUB, Marquard

Thousands of satellites are currently orbiting the Earth, and there will be many more in the future. Researchers from Ruhr University Bochum and the CISPA Helmholtz Center for Information Security in

Saarbrücken have assessed the security of these systems from an IT perspective.

They analyzed three current low-earth orbit satellites and found that, from a technical point of view, hardly any modern security concepts were implemented. Various security mechanisms that are standard in modern mobile phones and laptops were not to be found: for example, there was no separation of code and data. Interviews with satellite developers also revealed that the industry relies primarily on security through obscurity.

The results were presented by a team headed by Johannes Willbold, a Ph.D. student from Bochum, Dr. Ali Abbasi, a researcher from Saarbrücken, and Professor Thorsten Holz, formerly in Bochum, now in Saarbrücken, at the IEEE Symposium on Security and Privacy, which took place in San Francisco from 22 to 25 May 2023. The paper was awarded a Distinguished Paper Award at the conference.

Research satellites and commercial satellite put to the test

The examined satellites were two small models and one medium-sized model—research satellites as well as a satellite of a commercial company—which orbit the Earth at a short distance and are used to observe the Earth. Gaining access to satellites and their software was a challenge for the team, as commercial providers in particular rarely wish to reveal any details. The researchers eventually gained access through cooperation with the European Space Agency (ESA), various universities involved in the construction of satellites, and a commercial enterprise.

The team from Bochum and Saarbrücken conducted a thorough security analysis of the three models. They looked in detail at what the software

running on the devices does and which communication protocols are used. They emulated the systems, i.e., rebuilt them virtually, so that they could test the software as if it were in a real satellite. "It was a very different world from the systems we usually study. For example, completely different communication protocols were used," as Thorsten Holz outlines the process.

Moritz Schloegel (left) and Johannes Willbold analyzed the safety of satellites. Credit: RUB, Marquard

Systems with specific requirements

Satellites orbiting the Earth can only be reached by their ground station

on Earth within a time window of a few minutes. The systems must be robust against the radiation in space, and, since they can only consume a small amount of energy, they have a low power output. "The data rates are like those of modems in the 1990s," as Holz elaborates the challenges satellite developers face.

Based on the findings gained from the software analysis, the researchers worked out various attack scenarios. They showed that they could cut off the satellites from ground control and seize control of the systems, for example in order to take pictures with the satellite camera. "We were surprised that the technical security level is so low," points out Thorsten Holz, adding the following caveat with regard to potential ramifications: "It wouldn't be all that easy to steer the satellite to another location, for example, to crash it or have it collide with other objects."

Survey among developers

To find out how the people who develop and build satellites approach security, the research team compiled a questionnaire and submitted it to research institutions, the ESA, the German Aerospace Center and various enterprises. Nineteen developers participated anonymously in the survey. "The results show us that the understanding of security in the industry is different than in many other areas, specifically that it's security by obscurity," concludes Johannes Willbold.

Many of the respondents therefore assumed that satellites could not be attacked because there is no documentation of the systems, i.e., nothing is known about them. Only a few said that they encrypt data when communicating with satellites or use authentication in order to ensure that only the ground station is allowed to communicate with the satellite.

"However, a lack of documentation doesn't necessarily protect against attacks," points out Moritz Schloegel, co-author of the paper. "Today,

systems can be figured out through reverse engineering and their vulnerabilities can be identified. One of the goals of our project was therefore to bring the satellite and security communities together to promote a mutual understanding of the challenges of space applications and of the security standards that are in use today."

More information: Johannes Willbold et al, Space odyssey: An experimental software security analysis of satellites, (2023). DOI: 10.1109/SP46215.2023.00131. publications.cispa.saarland/39 … SatSec-Oakland22.pdf

Provided by Ruhr-Universitaet-Bochum