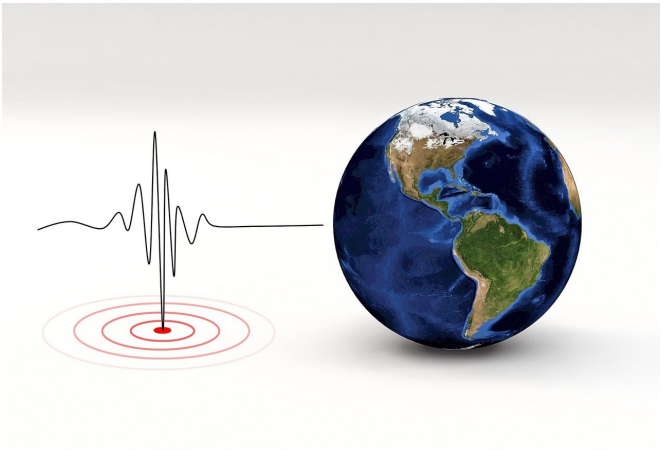
Tests reveal cybersecurity vulnerabilities of common seismological equipment

10 February 2021



Credit: Pixabay/CC0 Public Domain

Seismic monitoring devices linked to the internet are vulnerable to cyberattacks that could disrupt data collection and processing, say researchers who have probed the devices for weak points.

Common security issues such as non-encrypted data, insecure protocols, and poor user authentication mechanisms are among the biggest culprits that leave seismological networks open to security breaches, Michael Samios of the National Observatory of Athens and colleagues write in a new study published in *Seismological Research Letters*.

Modern seismic stations are now implemented as an Internet-of-Things (IoT) station, with physical devices that connect and exchange data with other devices and systems over the Internet. In their test attacks on different brands of seismographs, accelerographs and GNSS receivers, Samios and his colleagues identified threats to the equipment that information technology security professionals commonly find in IoT devices.

"It seems that most seismologists and network operators are unaware of the vulnerabilities of their IoT devices, and the potential risk that their monitoring networks are exposed to," said Samios. "Educating and supporting seismologists on information security is imperative, as in most cases unauthorized users will try to gain access through a legitimate user's computer to abuse monitoring networks and IoT devices."

By exploiting these vulnerabilities, a malicious user could alter geophysical data, slow down data transmission and processing, or produce false alarms in earthquake early warning systems, the researchers noted, causing the public to lose trust in seismic monitoring and potentially affecting emergency and economic responses to a seismic event.

Samios and colleagues launched a security assessment of seismic and GNSS devices attached to their own monitoring networks after a security incident at one of their seismic stations. There are several potential weak points in the security of these devices, they noted, including physical security in sometimes remote locations, difficulties and costs of updating security of hardware and software, usage of non-encrypted protocols, and default or easy login credentials.

Using their cybersecurity skills, the researchers tested these weak points using a typical "ethical hacking" process to surveil, scan and gain access to geophysical devices with their default settings. The most notable security issues, they discovered, were a lack of data encryption, weak user authentication protocols and the absence of a secure initial-default configuration

Samios and colleagues were able to demonstrate a launch of a successful denial-of-service or DOS attack against the devices, causing them to be unavailable for the period of the attack, as well as retrieve usernames and passwords for some of the

devices.

"Security weaknesses between different devices do not depend on the type of the device, but whether this device uses insecure protocols, outdated software and a potentially insecure default configuration," Samios said. "It is interesting, though, that while these vulnerabilities normally appear on low-cost IoT devices priced at $50 or less, it was also confirmed that they are observed even in seismological and GNSS devices that cost many times more."

As part of their tests, the research team was also able to intercept seismological data transferred through the SeedLink protocol, a data transmission service used by many seismologists. SeedLink may lack some of the necessary encryption and authentication protocols to keep data safe, Samios said. He noted that in a follow-up lab experiment not included in the SRL paper the researchers were able to manipulate waveforms transferred by SeedLink.

"This could potentially generate or conceal alarms on earthquake early warning and seismic monitoring systems, leading to disturbing situations," he said.

While device manufacturers and data transmission services should take steps to improve security functions such as data encryption, Samios said, seismic network operators can work with information security experts to help them develop safer user practices and enhance hardware and software systems.

More information: Michael Samios et al, Assessment of Information Security Vulnerabilities in Common Seismological Equipment, *Seismological Research Letters* (2021) doi.org/10.1785/0220200151