Horizon
The EU Research & Innovation Magazine

European Commission

Guardians of the grid – protecting Europe's electricity supply from cyber-attacks

EU-funded researchers are fortifying Europe's electricity sector against increasingly sophisticated attacks by cybercriminals.

03 October 2024 - By MICHAEL ALLEN

In the past decade, cyber-attacks on Europe's power infrastructure have intensified so much that energy companies, experts and politicians called for help. Researchers came together to boost the resilience of European energy networks.

The International Energy Agency warned in a November 2023 report that the average number of cyber-attacks against utilities worldwide more than doubled between 2020 and 2022. It singled out electricity grids, which are increasingly switching to digital technology.

"The technologies now deployed along electric grids make them vulnerable to issues with communication and information technology," said Jesús Torres, an expert in smart grids at the Spanish technology centre CIRCE.

Defending the grid

Torres leads a multi-country research initiative called eFORT that received EU funding to address the vulnerability of energy networks.

Researchers, energy companies and cybersecurity experts from Belgium, Cyprus, Germany, Greece, Italy, the Netherlands and Spain, plus Norway and Ukraine, are exploring ways to increase the reliability and resilience of power grids as Europe transitions to a fully digital system.

"The grid now has a double nature," said Torres. "It's an electrical system, but it's also a cyber system. Everything is digitalised, with sensors that can both monitor and control the grid."

That is why, since 2022, the eFORT team has been conducting simulations to understand how to protect electric grids from different kinds of cyber-attacks.

Simulating attacks

One particular area of concern is what Torres refers to as a “manipulation of demand” attack, when multiple internet-connected energy devices, like charging points for electric vehicles, are tricked into sending misleading information to the power grid.

For example, the grid might receive data indicating a lower demand for electricity than actually exists.

“The grid is then not configured for the actual demand, and this can lead to outages,” explained Torres.

The researchers’ simulations have shown that by targeting thousands of internet-connected devices, such attacks could trigger large-scale power cuts.

AI to the rescue

To counter attacks that corrupt information transmitted to the grid, the eFORT team is turning to artificial intelligence. The idea is to use algorithms to analyse grid communications and identify anomalies that signal potential issues.

Quick action is crucial once an attack is identified. In addition to shutting down affected grid elements, it may be necessary to isolate broader sections of the grid. By identifying these cascading effects, the eFORT researchers are designing targeted responses.

They are testing techniques to identify, prevent and mitigate grid disturbances in Spain, the Netherlands, Italy and Ukraine.

For instance, one Dutch pilot study includes a simulated control room where grid operators are trained to both defend against and emulate attacks, making them better able to manage threats.

AI also plays a central role in the three-year EU-funded ELECTRON project, which aims to make it possible to isolate grid sections to prevent the spread of attacks.

The ELECTRON team’s mission is to develop new-generation electricity platforms that will constantly assess cyber risks, detect anomalies and prevent failures.

Greek cybersecurity expert Andreas Zalonis, who coordinates this research, said that while there is often a financial motivation to these attacks, they can also be driven by a desire to destabilise society or create fear.

“There are a lot of different types of attack,” he said.

Along with ransomware attacks, where money is demanded to restore systems, Zalonis explained that economic motivations for attacks can also lie in the financial damage they can cause.

“For example, a power outage can have a significant financial cost for local companies, not just the energy and electrical system operators, and also for society,” he said.

The ELECTRON researchers hope to provide a series of tools to help European supply companies tackle cybersecurity issues.

They are conducting four pilot studies, including one inspired by the 2015 hacking of a power distributor in western Ukraine, which left more than 230 000 people without power.

Another study looks at cybersecurity risks to the Romanian power grid, which is powered by a mix of hydropower, coal, nuclear energy, natural gas and wind power.

The other two studies explore how to protect renewable energy supplies from cyber-attacks and test the resilience of an electric vehicle charging network in Greece.

The ELECTRON researchers are looking at everything related to a cyber-attack, from identifying parts of the grid most vulnerable to attack, through detecting and responding to attacks, to recovery after attacks.

AI is again being used to detect threats by monitoring information flows.

As part of these efforts, the researchers recently published information for electricity companies, highlighting the sort of communication anomalies that indicate someone might be interfering with the grid.

They are also distributing training materials, including attack scenarios, to help prepare those working on the grid. In addition, they are applying for patents for techniques that can be used to improve the security of electric vehicle charging points.

“The overall goal is always to increase the resilience of the infrastructure,” said Zalonis.

Research in this article was funded by the EU’s Horizon Programme. The views of the interviewees don’t necessarily reflect those of the European Commission. If you liked this article, please consider sharing it on social media.

More info

- ELECTRON
- eFORT
- EU network code on cybersecurity for the electricity sector
- EU Action Plan to digitalise the energy system
- The Digital Europe Programme