

Using physics to keep the electrical grid safe

October 25 2019, by Jessica Scully



Berkeley Lab researcher Sean Peisert. Credit: Marilyn Chung/Berkeley Lab

Many of the systems that provide services or products we use daily, such as the electrical grid, oil and gas pipelines, vehicles, and manufacturing

plants, are examples of cyberphysical systems—systems that integrate computing and networking with one or more physical components.

Computer security specialist Sean Peisert and a team of researchers at Berkeley Lab are helping ensure that these systems stay secure from cyberattacks. The team has collaborated with utilities and utility equipment companies on numerous projects to use the physical components of electrical grids—and the laws of physics they are subject to—to keep cyberattacks at bay.

Q. What makes cybersecurity different for a cyberphysical system than a computing system without a physical component?

A. Cyberphysical systems, such as the [power grid](#) and the components that control the [grid](#), have a physical consequence that most people are concerned about. It's not just somebody spying on your computer system or deleting some data. There's some sort of physical thing that a malicious actor can attempt to perpetrate. We looked at this and said, rather than viewing the physical connection of this system to the outside world simply as a liability, what if we could somehow leverage that physical connection and association as a benefit? Our projects revolve around using the laws of physics as an asset to our ability to secure systems rather than a liability that we have to worry about.

Q. How does the team's work use the laws of physics?

A. A normal computer system is fantastically complicated. It's really hard to define all good things and all bad things in advance. But the physical equipment that controls the power grid and even the power lines themselves have physical laws that govern their function. For example, physical laws govern the way electricity works. They govern the way

electrons flow across a wire. They govern what happens in terms of the temperature on the wire if you put too much electricity across it. They govern the way a rotating generator should spin. If something is physically behaving in a way that is antithetical to various laws of physics, like Ohm's law, Kirchhoff's law, and Newton's laws, then that gives us a much better indicator of what could be a cyberattack than the ways that we're usually able to detect attacks in traditional IT systems.

Q. Could you give an example?

A. Imagine an adversary was controlling whether or not we're getting power at will; that's kind of the nightmare scenario. Let's say somebody shuts off a substation that diverts the flow of electricity to another location. What happens then is the distribution line or transmission line starts heating up because it's getting more electricity than is expected. And so rather than detecting the actual cyberattack, we'd take notice of the fact that our sensors are telling us that more [power](#) is going across this particular line than should be.

Q. Could this approach be applied beyond power grids?

A. You could apply a similar sort of approach to just about any sort of computer-controlled physical system. It would require a different set of [laws of physics](#) and a different sort of model, and in chemistry and biology it might be an issue of properties and characteristics of how molecules and organisms interact rather than scientific laws. But with each you could imagine a similar approach of integrating safety engineering with computer security.

Provided by Lawrence Berkeley National Laboratory

Citation: Using physics to keep the electrical grid safe (2019, October 25) retrieved 8 May 2024 from <https://techxplore.com/news/2019-10-physics-electrical-grid-safe.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.