As ransomware attacks increase, new algorithm may help prevent power blackouts

October 5 2022, by Kayla Wiles

Saurabh Bagchi, a Purdue professor of electrical and computer engineering, develops ways to improve the cybersecurity of power grids and other critical infrastructure. Credit: Purdue University/Vincent Walter

Millions of people could suddenly lose electricity if a ransomware attack

just slightly tweaked energy flow onto the U.S. power grid.

No single power utility company has enough resources to protect the entire grid, but maybe all 3,000 of the grid's utilities could fill in the most crucial security gaps if there were a map showing where to prioritize their security investments.

Purdue University researchers have developed an algorithm to create that map. Using this tool, regulatory authorities or cyber insurance companies could establish a framework that guides the security investments of power utility companies to parts of the grid at greatest risk of causing a blackout if hacked.

Power grids are a type of critical infrastructure, which is any network—whether physical like water systems or virtual like health care record keeping—considered essential to a country's function and safety. The biggest ransomware attacks in history have happened in the past year, affecting most sectors of critical infrastructure in the U.S. such as grain distribution systems in the food and agriculture sector and the Colonial Pipeline, which carries fuel throughout the East Coast.

With this trend in mind, Purdue researchers evaluated the algorithm in the context of various types of critical infrastructure in addition to the power sector. The goal is that the algorithm would help secure any large and complex infrastructure system against cyberattacks.

"Multiple companies own different parts of infrastructure. When ransomware hits, it affects lots of different pieces of technology owned by different providers, so that's what makes ransomware a problem at the state, national and even global level," said Saurabh Bagchi, a professor in the Elmore Family School of Electrical and Computer Engineering and Center for Education and Research in Information Assurance and Security at Purdue. "When you are investing security

money on large-scale infrastructures, bad investment decisions can mean your power grid goes out, or your telecommunications network goes out for a few days."

Protecting infrastructure from hacks by improving security investment decisions

The researchers tested the algorithm in simulations of previously reported hacks to four infrastructure systems: a smart grid, industrial control system, e-commerce platform and web-based telecommunications network. They found that use of this algorithm results in the most optimal allocation of security investments for reducing the impact of a cyberattack.

The team's findings appear in a paper presented at this year's *IEEE Symposium on Security and Privacy*, the premier conference in the area of computer security. The team comprises Purdue professors Shreyas Sundaram and Timothy Cason and former Ph.D. students Mustafa Abdallah and Daniel Woods.

"No one has an infinite security budget. You must decide how much to invest in each of your assets so that you gain a bump in the security of the overall system," Bagchi said.

The power grid, for example, is so interconnected that the security decisions of one power utility company can greatly impact the operations of other electrical plants. If the computers controlling one area's generators don't have adequate security protection, then a hack to those computers would disrupt energy flow to another area's generators, forcing them to shut down.

Since not all of the grid's utilities have the same security budget, it can

be hard to ensure that critical points of entry to the grid's controls get the most investment in security protection.

The algorithm that Purdue researchers developed would incentivize each security decision maker to allocate security investments in a way that limits the cumulative damage a ransomware attack could cause. An attack on a single generator, for instance, would have less impact than an attack on the controls for a network of generators. Power utility companies would be incentivized to invest more in security measures for the controls over a network of generators rather than for the protection of a single generator.

Building an algorithm that considers the effects of human behavior

Bagchi's research shows how to increase cybersecurity in ways that address the interconnected nature of critical infrastructure but don't require an overhaul of the entire infrastructure system to be implemented.

As director of Purdue's Center for Resilient Infrastructures, Systems, and Processes, Bagchi has worked with the U.S. Department of Defense, Northrop Grumman Corp., Intel Corp., Adobe Inc., Google LLC and IBM Corp. on adopting solutions from his research. Bagchi's work has revealed the advantages of establishing an automatic response to attacks and has led to key innovations against ransomware threats, such as more effective ways to make decisions about backing up data.

There's a compelling reason why incentivizing good security decisions would work, Bagchi said. He and his team designed the algorithm based on findings from the field of behavioral economics, which studies how people make decisions with money.

"Before our work, not much computer security research had been done on how behaviors and biases affect the best defense mechanisms in a system. That's partly because humans are terrible at evaluating risk and an algorithm doesn't have any human biases," Bagchi said. "But for any system of reasonable complexity, decisions about security investments are almost always made with humans in the loop. For our algorithm, we explicitly consider the fact that different participants in an infrastructure system have different biases."

To develop the algorithm, Bagchi's team started by playing a game. They ran a series of experiments analyzing how groups of students chose to protect fake assets with fake investments. As in past studies in behavioral economics, they found that most study participants guessed poorly which assets were the most valuable and should be protected from security attacks. Most study participants also tended to spread out their investments instead of allocating them to one asset even when they were told which asset is the most vulnerable to an attack.

Using these findings, the researchers designed an algorithm that could work two ways: Either security decision makers pay a tax or fine when they make decisions that are less than optimal for the overall security of the system, or security decision makers receive a payment for investing in the most optimal manner.

"Right now, fines are levied as a reactive measure if there is a security incident. Fines or taxes don't have any relationship to the security investments or data of the different operators in critical infrastructure," Bagchi said.

In the researchers' simulations of real-world infrastructure systems, the algorithm successfully minimized the likelihood of losing assets to an attack that would decrease the overall security of the infrastructure system.

The research was published in the proceedings of the *2022 IEEE Symposium on Security and Privacy (SP)*.

More information: Mustafa Abdallah et al, TASHAROK: Using Mechanism Design for Enhancing Security Resource Allocation in Interdependent Systems, *2022 IEEE Symposium on Security and Privacy (SP)* (2022). DOI: 10.1109/SP46214.2022.9833591

Provided by Purdue University