Taking a systems approach to cyber security

March 2 2022

Credit: CC0 Public Domain

As critical infrastructure components such as electric power grids become more sophisticated, they are also becoming increasingly more reliant on digital networks and smart sensors to optimize their operations, and thus more vulnerable to cyber attacks. Over the past couple of years, cyber attacks on critical infrastructure have become

ever more complex and disruptive, causing systems to shut down, disrupting operations, or enabling attackers to remotely control affected systems. Importantly, the impacts of successful attacks on critical cyber-physical systems are multidimensional in nature, which means that impacts are not only limited to losses incurred by the operators of the compromised system, but also economic losses to other parties relying on their services as well as public safety or environmental hazards.

According to the study just published in the journal *Risk Analysis*, this makes it important to have a tool that distinguishes between different dimensions of cyber risks and also allows for the design of security measures that are able to make the most efficient use of limited resources. The authors set out to answer two main questions in this regard: First, whether it is possible to find vulnerabilities, the exploitation of which opens ways for several attack scenarios to proceed; and second, if it is possible to take advantage of this knowledge and deploy countermeasures to simultaneously protect the system from several threats.

One of the ways in which cyber threats are commonly managed is to conduct an analysis of individual attack scenarios through risk matrices, prioritizing the scenarios according to their perceived urgency (depending on their likelihoods of occurrence and severity of potential impacts), and then addressing them in order until all the resources available for cybersecurity are spent. According to the authors, however, this approach may lead to suboptimal resource allocations, given that potential synergies between different attack scenarios and among available security measures are not taken into consideration.

"Existing assessment frameworks and cyber security models assume the perspective of the operator of the system and support her cost-benefit analysis, in other words, the cost of security measures versus potential losses in the case of a successful cyber attack. Yet, this approach is not

satisfactory in the context of security of critical infrastructure, where the potential impacts are multidimensional and may affect multiple stakeholders. We endeavored to address this problem by explicitly modeling multiple relevant impact dimensions of successful cyber attacks," explains lead author Piotr Żebrowski, a researcher in the Exploratory Modeling of Human-natural Systems Research Group of the International Institute for Applied Systems Analysis (IIASA) Advancing Systems Analysis Program.

To overcome this shortcoming, the researchers propose a quantitative framework that features a more holistic picture of the cyber security landscape that encompasses multiple attack scenarios, thus allowing for a better appreciation of vulnerabilities. To do this, the team developed a Bayesian network model representing a cyber security landscape of a system. This method has gained popularity in the last few years due to its ability to describe risks in probabilistic terms and to explicitly incorporate prior knowledge about them into a model that can be used to monitor the exposure to cyber threats and allow for real-time updates if some vulnerabilities have been exploited.

In addition to this, the researchers built a multi-objective optimization model on top of the Bayesian network that explicitly represents multiple dimensions of the potential impacts of successful cyber attacks. The framework adopts a broader perspective than the standard cost-benefit analysis and allows for the formulation of more nuanced security objectives. The study also proposes an algorithm that is able to identify a set of optimal portfolios of security measures that simultaneously minimize various types of expected cyber attack impacts, while also satisfying budgetary and other constraints.

The researchers note that while the use of models like this in cyber security is not entirely unheard of, the practical implementation of such models usually requires extensive study of systems vulnerabilities. In

their study, the team however suggests how such a model can be built based on a set of attack trees, which is a standard representation of attack scenarios commonly used by the industry in security assessments. The researchers demonstrated their method with the help of readily available attack trees presented in security assessments of electric power grids in the US.

"Our method offers the possibility to explicitly represent and mitigate the exposure of different stakeholders other than system operators to the consequences of successful cyber attacks. This allows relevant stakeholders to meaningfully participate in shaping the cyber security of critical infrastructure," notes Żebrowski.

In conclusion, the researchers highlight that it is important to have a systemic perspective on the issue of cyber security. This is crucial both in terms of establishing a more accurate landscape of cyber threats to critical infrastructure and in the efficient and inclusive management of important systems in the interest of multiple stakeholders.

More information: Piotr Żebrowski et al, A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems, *Risk Analysis* (2022). DOI: 10.1111/risa.13900

Provided by International Institute for Applied Systems Analysis