Case Study with Supporting Media and Simulation Exercise

Title: Inverter-Based Security Threats to Solar Energy Resources

Real World Inspiration

In May 2024, a Japanese industrial control electronics manufacturer confirmed that cyber attackers hijacked 800 SolarView Compact remote monitoring devices at solar power generation facilities. Attackers exploited a command injection vulnerability in systems that had not been patched. The objective of the attack was financial exploitation. This incident may be the first publicly confirmed cyberattack on the solar power grid infrastructure. While the exploitation of SolarView remote monitoring devices in this specific attack did not disrupt the power grid operations, intrusion via inverters, a vital component in solar power installations, is a likely vulnerability through which attacks on operational technology in the power grid infrastructure can occur [1].

(a) Distributed Energy Resources and Photovoltaic Systems

Distributed Energy Resources (DER) are small energy generation and storage technologies that provide electric capacity or energy. DER systems may be either connected to the local electric power grid or isolated from the grid in stand-alone applications, such as for household-use. DER technologies include photovoltaics (PV) generation systems. DER technologies have been growing in popularity over the years due to their minimal environmental impact and are being integrated into the larger power grid, replacing many traditional power generation sources. Solar panel installations are a type of DER and are made up of photovoltaic cells. PV cells are thin layers of a semiconductor material that converts sunlight directly to DC electricity. PV systems are different from traditional power generation sources because they require power electronics to convert its output current from DC to AC in order to regulate the flow of the generated power [2].

(b) Inverters

An inverter is a type of power electronic system that regulates the flow of electrical power. Solar panels produce direct current (DC) electricity, which has a constant voltage in one direction, like how a battery works. Inverters are responsible for converting DC into alternating current (AC) electricity, to incorporate solar panel installations into the electrical grid. Traditional power generation relies on rotating equipment like an electric generator, producing AC power as the device rotates. This makes inverters unique to solar power and can introduce new attack avenues for cyber actors to exploit [3].

In household solar systems, inverters often perform several functions on top of converting solar energy into AC power including monitoring the system and providing a portal for communication with computer networks [4]. Inverters are becoming more advanced due to their monitoring and control capabilities which require an internet connection, which increases the risk for a cyberattack [5]. A connection to the internet is both a convenience and a major vulnerability to a system since the internet allows for the system to be potentially accessed from anywhere in the world. Solar power installations are a component of the modern electric grid that make it a cyber-physical system, which has both software and physical components. In a cyber-physical system, an attacker gaining access from the IT portion of the system can result in physical repercussions, in this case things like loss of power and fires [5]. Solar panel infrastructures and their inverter-based interfaces between the operational technology and software components are becoming increasingly interconnected with the larger power grid, presenting a risk of power grid disturbances [3].

(c) Applicable CIE Principles

Cyber-Informed Engineering (CIE) is an engineering approach that integrates cybersecurity considerations into the conception, design, build, and operation of any physical system that has digital connectivity, sensors, monitoring, or control [6]. Cyber-Informed Engineering principles must be incorporated in the design and deployment of solar power infrastructures as new solar power technologies are integrated into the power grid. As the electric grid is increasingly digitalized and connected, solar energy installations are vulnerable to cyberattack through the exploitation of solar panel inverters. As inverters become advanced and are used for monitoring and control, they act as the interface between solar panels and the grid. This provides utilities with real-time solar power generation and other information, meaning they must be secured [4].

Attacks on inverters can affect critical electrical infrastructure because they can be injected with false data or malicious code, which can spread malware into the larger system [5]. CIE Principle 1, **Consequence-Focused Design**, asks engineers to consider where “an unprotected action or failure of the function that leverages digital technology might lead to a high-consequence event” [6]. These could include unauthorized system actions and invalid data that would drive an automated action [6]. Utilities can and should try to prevent attackers from injecting false information with security software. Additionally, implementing engineering controls like strictly defining ranges of values for each of the parameters that define critical grid-support functions, like voltage, frequency, and power values, should be configured to fall within specific ranges that ensure the function provides desired power system behavior [3].

Unauthorized and false commands in solar panel inverters can cause cyber-physical security breaches, like a change in current or voltage that is injected into the electric grid [4]. CIE Principle 6, **Active Defense**, asks that engineered systems “employ real-time active capabilities and preplanned contingency actions to deter, detect, and delay cyber threat activity, enabling critical functions to continue operating resiliently until the threat has been neutralized and normal functionality is recovered” [6]. Tools in the PV network should visualize and capture real-time data from control networks to detect threats [3]. One control that can detect changes in real time and help to maintain the critical electrical infrastructure of the larger grid during the incident of a security breach is a digital twin. Digital twins are digital representations of physical systems that instantaneously monitor and forecast solar farm system behavior [7]. When used for risk management and cyber intrusion detection, digital twins can provide dynamic assessment of the threat and have situational awareness of the attack’s impacts on PV systems’ operational technologies. Then, utilities can respond and recover, by using other power generation sources if the PV network is compromised in order to maintain critical functioning of the grid [3].

CIE Principle 3, **Secure Information Architecture**, prompts engineers to segregate important data to minimize network vulnerabilities. Because inverters provide a communicable interface between the utility and the equipment, this poses a significant risk through communication channels including the open internet. Mechanisms include network segmentation, which protects critical functions from outsider view [6]. Parts of the Industrial Control System (ICS) network should be segmented with VPNs and firewalls; however, PV systems face additional challenges with traditional network enclaving methods. Because not all networks are owned by a single entity, particularly in residential and commercial PV systems, communications are established through the public internet. However, with networks that are owned by the grid operator, it may be possible to enclave the devices if communications are passed directly to the solar farm through single-entity-owned networks through dedicated SCADA networks to utility-owned PV systems [3]. PV control networks can also be secured against cyberattack by rotating network addresses, network parameters, and application libraries. This approach uses software defined networks (SDN) to eliminate a class of adversaries that rely on known static addresses for critical infrastructure network devices [3].

CIE Principle 5, **Layered Defenses**, assumes the system can be compromised and employs a defense-in-depth strategy [6]. Defense-in-depth strategies are recommended, as standards alone cannot protect critical infrastructure. Industry should proactively conduct cyber security evaluations, require good cyber security hygiene, rapidly patch systems, mitigate the insider threat, and address supply chain risks [3]. The best overall approach to security is to consider all the CIE principles in the different stages of the engineering process in order to create this layered defense and provide ample security to the system.

Media Feature for the General Audience

For a custom media clip designed by faculty and students of the University of Pittsburgh, please click on the video file found here: Team Anaconda Media Feature

This video has a casual and fun approach to it, as it starts off with a cold-open-style skit designed to engage audiences, specifically students, in a humorous manner.

According to AACSB, "A well-conceived, thoughtful, and funny three-to-five-minute [educational comedy] can provide enough colorful examples, metaphors, and memes to sustain a lively discussion for up to 90 minutes as participants keep returning to and building on ideas. In addition, the shared fun experience provides a social lubricant that helps create a positive atmosphere conducive to learning [8]." This emphasizes the positive effects that humorous educational videos can have and how they can bring complex topics to life in entertaining ways. This is applied in this video, as it explains how although solar power energy is new, advanced, and exciting, people often overlook the potential risks and vulnerabilities that might come along with it.

Future Policy Implications

As the electrical grid turns toward sustainable energy sources, there is growing concern of the increased susceptibility to cyberattacks. Inverter-based resources (IBR) play a pivotal role in this sustainability transformation and are vital in protecting against cyberattacks. According to the North American Electric Reliability Corporation (NERC), IBRs may be defined as Bulk Power Supply (BPS) connected facilities that have a power interface between the AC grid and the source of electricity. Consequently, IBRs are integral in this turn toward sustainable energy sources as they include solar arrays, modern wind turbines, and battery storage resources. Nevertheless, as the amount of power generated by IBRs increases, a reliability gap has emerged where a significant amount of BPS-connected IBR owners and operators were not yet required to be registered with NERC or adhere to NERC's reliability standards. As a result, the Federal Energy Regulatory Commission (FERC) issued an order for NERC to identify and register these owners and operators. Nonetheless, this highlights how reliability should be a key focus of policy and organizational concerns, specifically regarding solar power and inverter vulnerabilities. Therefore, it is critical for policy to address these concerns as the grid transforms through BPS-connected IBRs, fostering greater risk to grid reliability. In turn, these risks may be framed as a contingency, one that may ultimately hinder the expansion of renewable energy resources.

Consequently, one must consider the organizational structures of vendors and utilities and examine ways in which operational processes can be changed to reflect the growing concern of cybersecurity and sustainability. However, there has been limited progress in DER cybersecurity work to date [3]. Therefore, to address concerns specifically related to solar power, one must spur greater funding and research into DER cybersecurity, as this provides the foundations for further cybersecurity advancements regarding sustainability and "green" resources. Despite this limited progress, it is important to propose possible policies that aim to mitigate potential cybersecurity risks specifically related to solar power systems. An overarching approach is through the idea of "stakeholder engagement," which is vital in developing and improving existing solar power communication systems, an area that is often susceptible to cyber threats [3]. Stakeholder engagement features varied methods of strengthening communication across industry, government, and academia. Some of these methods include regular auditing, creating continuity plans, and implementing practices that may be scaled within an organizational environment, all to assess the existing security network. Furthermore, the most integral part of stakeholder engagement is information sharing. Although there are often complications of sharing cyber threat information, information sharing between industry, government agencies, and academic experts to grid operators is critical in bolstering communication and preventing any compartmentalization that may hinder cyber security advancements. Perhaps most ambitiously, there may be a new cybersecurity information-sharing network that is unique to DER systems, so that when an attack on a solar power system occurs, the information regarding the attack method may be disseminated to all stakeholders. In order to improve grid reliability and to adapt to the rapid development of DER devices and other sustainable resources, stakeholder engagement and information sharing remain pivotal decisive policy approaches.

Part 1: Expand Your Understanding with the Following Exercise

(a) Hypothetical Scenario 1: A homeowner wants to be more eco-friendly by switching to renewable energy instead of the coal and natural gas that had been powering and heating their home. This homeowner has decided that they want to purchase and install a solar energy system on their home, hoping that the investment in their own panels will reduce the cost of electricity to save them money in the long term. Unbeknownst to the homeowner or the solar panel company, a recent firmware update that was pushed to all this company's inverters which resulted in a vulnerability in the software for the controls. An attacker who wants to give the solar company a bad reputation since they have invested in several oil companies has discovered this vulnerability. The attacker gains control of the system through this vulnerability and was able to disconnect the power from the house.

a. Question 1: CIE Principle 1 is **Consequence-Focused Design**, which stresses understanding the critical functions of the system and what undesired consequences must be prevented [6]. What are some of the consequences of power loss in a home? In this scenario, what are some other consequences that could have resulted from an attacker having access to the controls of the inverter?

b. Question 2: CIE Principle 10 is **Planned Resilience**, which asks the engineer to plan for the possibility of critical functions failing due to a cyber-attack and create conditions for continued operations under those circumstances [6]. What are some fail safes that an engineer could add to this home solar power system to prevent damage?

c. Question 3: What are the pros and cons of having a home solar power system connected to the internet? Consider what CIE principles are applicable to both sides of this question when answering [6].

(b) Hypothetical Scenario 2: Assume that, in this scenario, there is again a firmware update to all the inverters owned by a solar power company that results in a vulnerability in the software for the controls. This time, the attacker attacks a solar panel farm remotely. The attacker is patient and gains access to the controls of all the inverters. In quick succession, the attacker disconnects the power at these inverters. This results in an outage to the community that relied on the power generated at the solar farm.

a. Question 1: What are the consequences of this attack on the farm and the blackout? Discuss the difference in scale between the consequences of an attack like the first hypothetical scenario with a single home solar power vs an attack a whole solar farm.

b. Question 2: As solar farms and other inverter-based resources are increasingly highlighted as areas of cybersecurity concern, what are some potential organizational policies that may ensure a plan for active defense?

c. Question 3: CIE Principle 5 is **Layered Defenses**, which discusses using a compilation of defense strategies to reduce the opportunity for a single failure to impact critical functions [6]. What are some of the ways that a layered defense could be built to minimize the effects seen in Hypothetical Scenario 2?

Further Reading and Useful Public Video Links

For further reading, the following references would be suitable to explore at your convenience.

[1] "Hijack of monitoring devices highlights cyber threat to solar power infrastructure," CSO Online. https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html

[2] "Using Distributed Energy Resources: A How-To Guide for Federal Facility Managers Distributed Energy Resources: A How-To Guide." Available: https://www.nrel.gov/docs/fy02osti/31570.pdf

[3] J. Johnson, "Roadmap for Photovoltaic Cyber Security," Sandia National Laboratories, 2017. [Online]. Available: https://www.researchgate.net/profile/Jay-Johnson-11/publication/322568290_Roadmap_for_Photovoltaic_Cyber_Security/links/5accfd764585154f3f3f9f9b/Roadmap-for-Photovoltaic-Cyber-Security.pdf

[4] Office of Energy Efficiency & Renewable Energy, "Solar Integration: Inverters and Grid Services Basics," Energy.gov. https://www.energy.gov/eere/solar/solar-integration-inverters-and-grid-services-basics

[5] "Solar Cybersecurity Basics," Energy.gov. https://www.energy.gov/eere/solar/solar-cybersecurity-basics

[6] V. L. Wright et. al., "Cyber-Informed Engineering Implementation Guide," United States, 2023. Available: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

[7] G. Writer, "How digital twins can mitigate operational risk for wind and solar projects," *Infrastructure Investor*, Jan. 09, 2024. https://www.infrastructureinvestor.com/how-digital-twins-can-mitigate-operational-risk-for-wind-and-solar-projects/#:~:text=Dialling%20down%20cyber%2Drisk

[8] "Using Comedy to Teach Serious Business | AACSB," www.aacsb.edu. https://www.aacsb.edu/insights/articles/2021/07/using-comedy-to-teach-serious-business

Authors

Erin Clark is a rising junior studying Communication Rhetoric, along with a minor in Spanish Language and a certificate in Television and Broadcast Arts. She has previous experience in the world of media, including work with anchoring, reporting, producing, interviewing, and hard-news broadcasting.

Abby Magistro is a rising senior computer engineering major. She has experience with cyber-security and simulations from her coursework, and plans to learn more about cyber-security, cyber-physical systems, and software development throughout her senior year to help her pursue a career in one of those fields.

James Ross is a rising senior studying History and Political Science and pursuing a certificate in Public and Professional Writing. He plans on pursuing graduate study in public policy and international affairs.

Amy Zhang is a rising junior majoring in Information Science and Digital Narrative and Interactive Design, with a minor in Computer Science. She has experience in journalism and storytelling through digital interface and is interested in the implications of increased digitalization of physical systems.