Vulnerabilities of the American Power Grid

Nicholas Metzger

Mentored by Ming Chow

Tufts University

December 13, 2017

Abstract

Electricity has become a crucial aspect of our lives that is responsible for many of the modern conveniences provided for us. We use electricity to refrigerate and cook our food, power our laptops, iPads and smartphones, to control street lights to direct traffic, to heat our homes, to provide light to our homes, streets, and towns, and so much more. Electricity is necessary for even more essential aspects such as defense, transportation, and communication.

The loss of electricity due to snowstorms, hurricanes, earthquakes, or other natural disasters cause states of emergencies because we rely so heavily on electricity. Now hackers have successfully attacked and continue to attempt to disrupt our power grid. Ukraine has suffered from repeated attacks on its power grid in both 2015 and 2016 [6], and now America may be the next victim of a power grid attack: a recent report in September from a Cyber Security firm called Symantec says that hackers have already successfully infiltrated US energy companies.[5]

How have hackers been able to breach nuclear power plants, solar panels and power companies? Is there a possibility for a widespread induced blackout by a hostile nation or group of individuals? What can be done to prevent future attacks on our power grid? What can be done to minimize fallout from a future attack? These questions will be answered here.

Introduction

Before we dive into the vulnerabilities of the electric grid, we need to define what is the electric grid. According to studentenergy.org, the "electrical grid is the means through which power is generated, transmitted, and distributed to the end user."[2] However, what comprises the electric grid?

Three main components exist which make up the modern power grid. Generators such as nuclear power plants, solar panels, and coal-burning power plants, create electricity. Utility companies control and own these electricity generators, however they are closely monitored by a state's Public Utility Commission or Public Service Commission. Transmission lines, either overhead power lines or underground power cables, carry high-voltage electricity from generators to consumers. Why don't transmission lines transport less dangerous, lower-voltage electricity? The higher the voltage, the less amount of electricity is lost. Finally, the distribution network converts high-voltage electricity into low-voltage electricity through transformers, and delivers usable electricity to consumers.[1] Having identified the crucial components of the power grid, how can a power grid be susceptible to a cyber attack?

The most prevalent and fortunately least harmful attacks are network hacks, in which hackers gain access to company emails, computers, and web servers. These types of attacks are usually instigated by spear phishing emails or watering hole attacks.[7] Spear phishing emails are emails that have been cleverly crafted by hackers to appear to be legitimate however contain malware or a link to a website with malware.[9] The other primary method of attack, a watering hole, steals data or gives a virus to a user's computer. A hacker will target an individual, monitor

and determine commonly visited websites by that individual, find a vulnerability in that website, and finally using that vulnerability redirect the individual to a website laced with malware.[10]

Hackers gaining access to operational technology systems of a power grid is a much more consequential attack. The operational technology systems (OT) of a power grid are what actually control the physical power equipment. In theory, OT systems should have no network communications with IT systems, but with exception of nuclear power plants, co-founder of security firm Claroty, Galina Antova says she is always able to find a path between OT and IT systems.[7]

Finally, the ultimate goal a hacker would desire is a coordinated attack on an electric grid. With operational access, knowledge of the system, and a plethora of time, resources and planning, hackers have the ability to perform a coordinated attack on a power grid. If hackers were to do this severe attack on the American power grid, “hackers [would] have to choose between scope and duration of blackout.”[7]

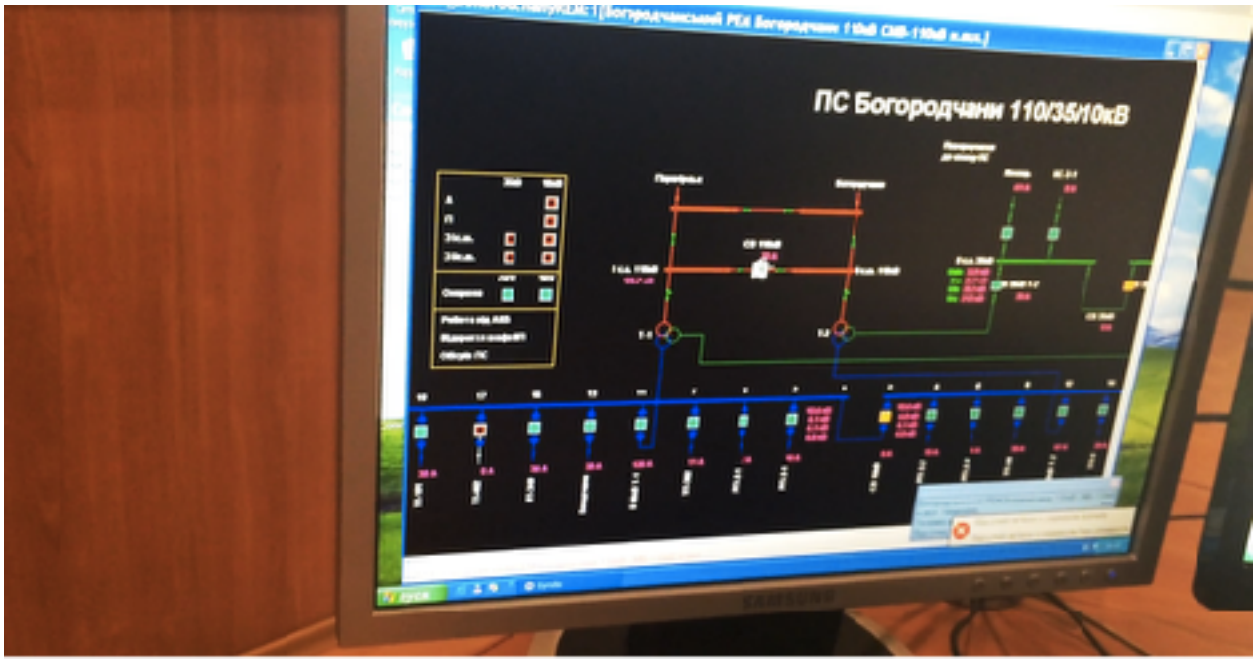
To the Community

Incidents over the past few years have revealed the looming and ever more likely possibility of a coordinated attack on the American power grid. And unfortunately, the United States may already be at the mercy of a severe cyber attack on its power grid.

Induced Blackouts in Ukraine

Twice, in 2015 and 2016, hackers induced blackouts in Ukraine affecting millions of people. Each only lasted a few hours, but the fact that they occurred at all is quite alarming. It was determined that multiple Ukrainian power companies had been infected by a Microsoft Word attachment, which had run a script, infecting a multitude of other machines without raising suspicion, and eventually the companies' networks and a VPN which had been used to gain remote access to their networks.[6]

Why does these events matter? Just because hackers were able to control and turn off the power for most of Ukraine doesn't mean that it will happen to the United States. Well, both yes and no. The United States and Ukraine surely are not the same and these specific attacks would probably not affect the United States' power grid, however it shows that inducing a mass blackout is no longer just an idea, but is a real, tangible possibility and can potentially occur in the United States.[6]



Above, a computer in a Ukrainian power company whose mouse is being remotely controlled by a hostile agent.[8]

Solar Panel Vulnerabilities

In August of 2017, Willem Westerhof, a cybersecurity researcher at ITsec, found 21 vulnerabilities in solar panels created by German specialists SMA Solar Technology. The vulnerabilities arise specifically from power inverters, which transform direct current from solar panels to alternating current to be supplied to the power grid. Hackers can exploit this if they were connected to same network as the equipment. With enough solar panels supplying a power grid, hackers could induce a blackout if they either overflowed or underflowed the grid with energy.[3]

Some of the 21 bugs in the inverters included having a weak password policy since there was no complexity or length requirements. Additionally, passwords were sent unencrypted as

they were typed into corresponding software Sunny Explorer, and thus able to be viewed if a hacker were to sniff the transferred packets.[3]

After the vulnerabilities were identified, SMA Solar Technology fixed these problematic issues. However, this incident is telling of how as new technology is utilized to create more and/or greener energy, vulnerabilities exist and can have a severe impact on a power grid.

Nuclear Power Plant Network Hack in Wolf Creek, Kansas

Administrative and business networks of the Wolf Creek Nuclear Operating Corporation were hacked in the summer of 2017, but no operational systems had been affected. Part of the attack seemed to gather intel on computer networks for future attacks. Most of the attacks targeted people who had direct access to systems that if damaged, could result in fire, explosion, or toxic spill. The hackers' techniques appeared similar to those of Energetic Bear, a Russian hacking group.[4]

Hackers used spear phishing emails to gather sensitive data. More specifically, hackers sent emails appearing to be resumes but really containing exploitive code to senior industrial control engineers, who had control to various operating control systems. Once the engineers opened the malicious documents, the hackers stole engineers' credentials. Watering hole attacks and man in the middle attacks were also performed.[4]

Fortunately, hackers did not gain access to industrial control systems, however these attacks were a clear sign that hostiles are attempting to breach the American energy sector.

Hackers Gain Access to American Power Grid Controls

Security firm Symantec in August of 2017 warned that after recent attacks, hackers now have operational access of the power grid. Symantec identified the hacker group Dragonfly 2.0 as the ones responsible for infiltrating more than 20 energy companies' networks and gaining access to the operational systems of some of these companies.[5]

Attacks included spear phishing emails that were actually fake invitations to a New Year's Eve party and watering hole attacks in which the frequently visited websites of a victim are compromised in order to hack the victim's machine. With these attacks, hackers were able to obtain usernames and passwords and from there gain access to the victims' machines to take pictures of operational control panels.[5]

The attacks were so serious that Eric Chien, a Symantec security analyst, reported "We're now talking about on-the-ground technical evidence [sabotage of the power grid] could happen in the US, and there's nothing left standing in the way except the motivation of some actor out in the world."[5]

Action Items

With all of these stunning revelations, one would probably ask, “I don’t work at an energy supplier or power company so how am I able to help make a difference in securing our power grid?” There are a multitude of things you can and should do.

Firstly, get informed. Perform research into your energy supplier and distributor: call a representative and find out if these companies consider cyber security a high priority. Ask what they have done to mitigate and prevent possible future attacks. Demand of your energy companies to hire cyber security professionals to train and teach its employees about the real, looming threats of attacks on our power grid and what measures can be taken to prevent these attacks.

Next, if the company appears to be unconcerned with cyber security or procrastinating handling these current critical issues, then you should find business in a new energy company. Nothing talks more than money. Boycott these companies and inform them that your decision to leave them is based on their lack of concern with the tangible threats towards the energy grid. Your voice can make a difference, and if companies, apathetic to cyber security, see enough of a loss in revenue, they will start to listen and will quickly become more attentive on securing the electrical grid.

Finally, write to your congressman to urge the United States Government to prioritize defending the American power grid from domestic and foreign attacks. The power grid is a service that provides crucial power and structure to the entire country; the government should and must be invested in defending the power grid. Since power companies have refused to take responsibility for their lack of urgency and awareness, with the help of government intervention,

power companies can be forced to reconcile for their egregious inaction and begin to prioritize protecting the American power grid.

Conclusions

Hackers inducing blackouts is now a reality that America must prepare for. Blackouts have been caused before in Ukraine twice, and hackers continue to attempt to disrupt the American power grid, and now potentially are able to coordinate a planned attack ever since hackers have retrieved operational access to parts of the grid. Would these power outages be sustained for a long period time? Most likely not. However, they would pose a serious threat to both the national security of our country and to the American people's faith in our energy companies and the government.

References

1) How the Electricity Grid Works. (n.d.). Retrieved December 13, 2017, from http://www.ucsusa.org/clean-energy/how-electricity-grid-works#.WfqXaBNSyGQ
2) Electrical Grid. (n.d.). Retrieved December 13, 2017, from https://www.studentenergy.org/topics/electrical-grid
3) Iain Thomson in San Francisco 7 Aug 2017 at 21:19 tweet_btn(). (n.d.). Hackers could exploit solar power equipment flaws to cripple green grids, claims researcher. Retrieved December 13, 2017, from https://www.theregister.co.uk/2017/08/07/solar_power_flaw/
4) Perlroth, N. (2017, July 06). Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say. Retrieved December 13, 2017, from https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?_r=0
5) Greenberg, A. (2017, September 06). Hackers Gain Direct Access to US Power Grid Controls. Retrieved December 13, 2017, from https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/
6) Greenberg, A. (2017, June 19). How An Entire Nation Became Russia's Test Lab for Cyberwar. Retrieved December 13, 2017, from https://www.wired.com/story/russian-hackers-attack-ukraine/
7) Greenberg, A. (2017, November 01). How Power Grid Hacks Work, and When You Should Panic. Retrieved December 13, 2017, from https://www.wired.com/story/hacking-a-power-grid-in-three-not-so-easy-steps/
8) Greenberg, A. (2017, June 20). Watch Hackers Take Over the Mouse of a Power-Grid Computer. Retrieved December 13, 2017, from https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/
9) (n.d.). Retrieved December 13, 2017, from https://usa.kaspersky.com/resource-center/definitions/spear-phishing
10) Web Injection Process Used in Watering Hole Attacks. (n.d.). Retrieved from https://www.symantec.com/content/en/us/about/media/pdfs/b-istr_18_watering_hole_edits.en-us.pdf