Security Assessment of Distributed Energy Resource Inverter

Sophia McMahon, Keaton Persons, Ben McCornack

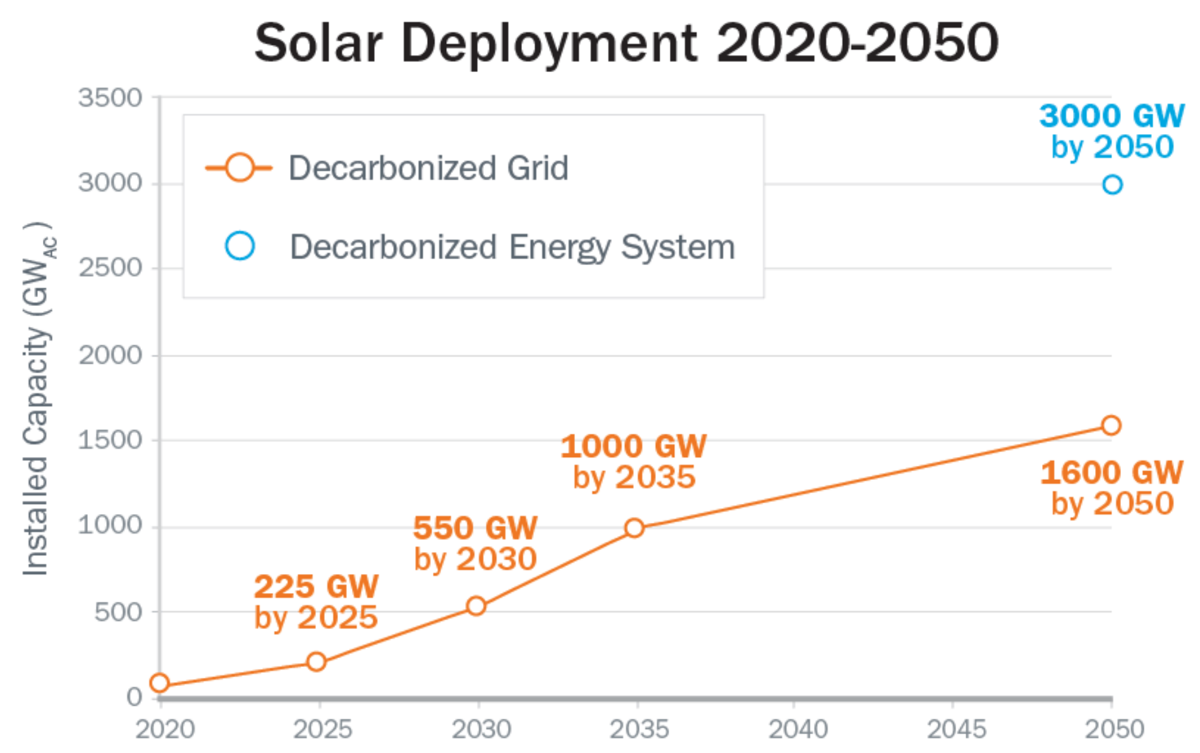
INTRODUCTION

There has been a significant rise in the number of smart inverters being installed onto the power grid. Smart inverters are what connect renewable energy sources such as solar panels and batteries. While these sources are great for establishing a new sustainable future. It is causing a new cyber security challenge.

Traditionally generation was owned by large and incentivized utility companies that have a great interest in keeping their sites and networks secure. With this push into a renewable future, much of the power generation is now owned by individual public entities. These entities individually provide an inconsequential amount of power and likely don't have the same need or care for cyber security as a utility may.

Adversaries will most likely have a much easier time collecting a host of unsecure smart inverter-based resources than they would taking control of a control center of a utility.

This project explores methods and attack vectors that have been proven to work against commercial inverters that are on the market today.



Source

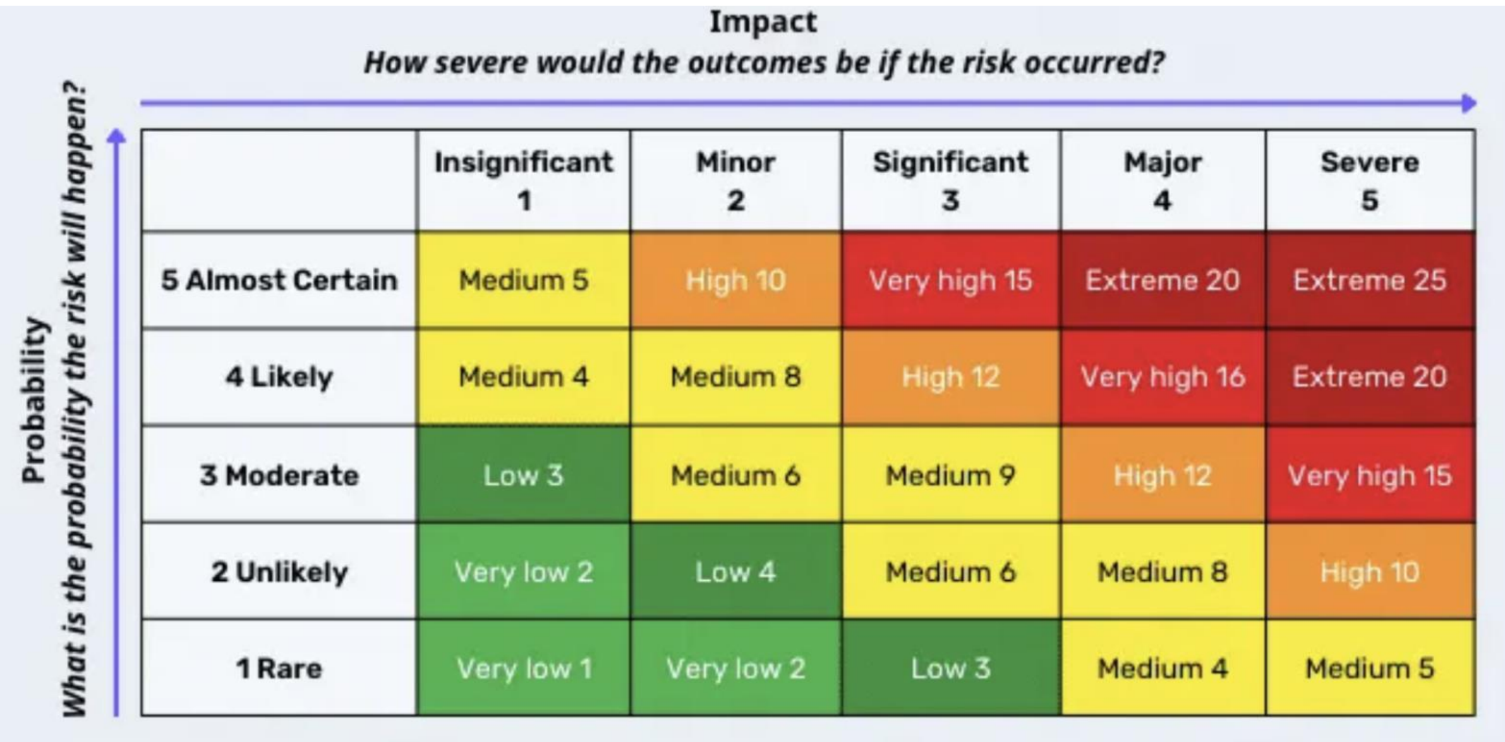
CONSIDERATIONS

Would an adversary attack the grid?

Before moving forward, it is worth discussing the validity of this concern. There seems to only be one reported hack against a power grid that happened in 2015 in Ukraine where it was suspected that the adversary was Russia. Source

With so little precedent, why should we be concerned with the cyber security of small power system devices? The concerns that make this kind of attack worth of study is not due to financial or reputation reasons. The value of this study is due to the magnitude of repercussions if an adversary were to be successful in such an attack.

Today, utilities are responsible for maintaining a constant supply of high-quality power to our homes, businesses, but more importantly our critical infrastructure such as water treatment and hospitals. For every inverter installed, the utilities lose that much more of their ability and authority in being responsible for the reliability of our power.

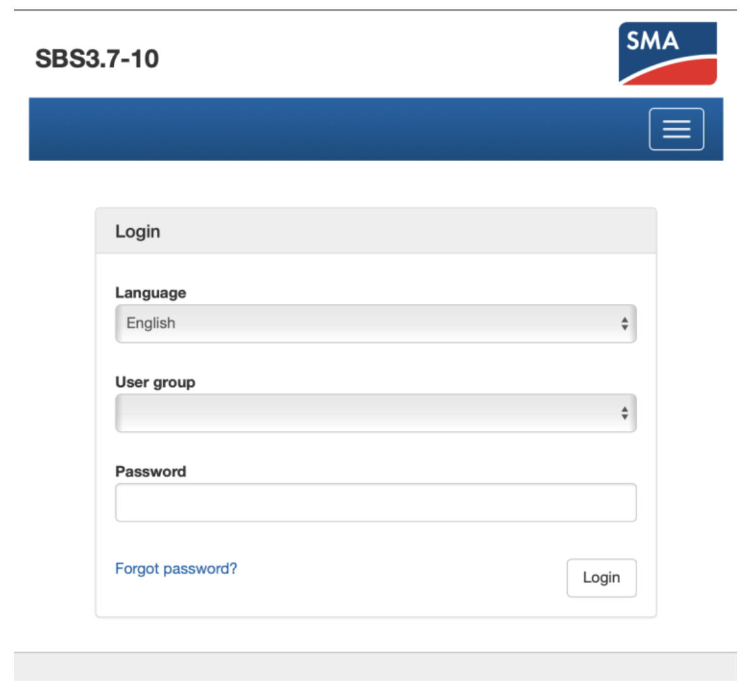

Impact
How severe would the outcomes be if the risk occurred?
Probability
What is the probability the risk will happen?

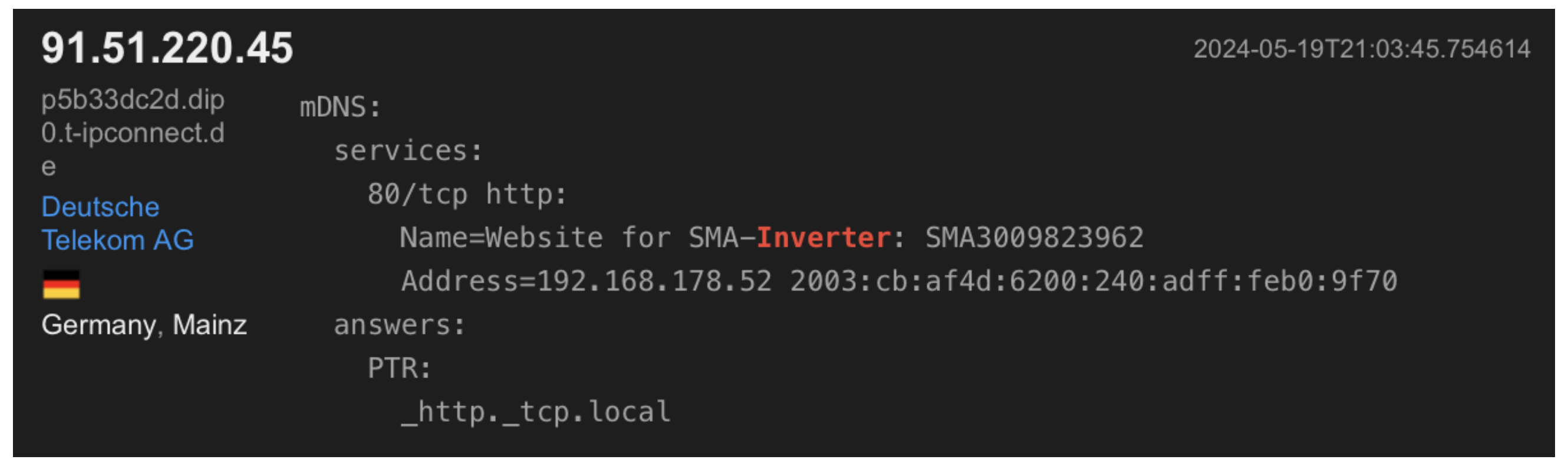
	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Fig 1. Impact Vs. Probability [1]

Exposure

Using a website named showdan.io. It only takes a simple search of "inverter"' to view the ip addresses of a few hundred inverters across the world. This is not a sophisticated search through the exposed ip and ports on the internet and yet it revealed that there are smart inverters open on the internet.





```
91.51.220.45                                        2024-05-19T21:03:45.754614
p5b33dc2d.dip    mDNS:
0.t-ipconnect.d    services:
e                    80/tcp http:
Deutsche               Name=Website for SMA-Inverter: SMA3009823962
Telekom AG             Address=192.168.178.52 2003:cb:af4d:6200:240:adff:feb0:9f70
                   answers:
Germany, Mainz       PTR:
                       _http._tcp.local
```

Fig 2. Exposure on Showdan.io [2]

METHODS

How would the adversary gain access?

Most papers assume that the adversary already has access to the inverter from within a network. Some methods that have been implemented with this assumption are summarized below.

- **SSH + Brute Force:** A cheap and easy to implement attack that is made possible when a device doesn't have a limit to the number of login attempts. Combining this tool with a search engine such as showdan.io that returns exposed ip addresses on the internet makes for a simple attack.
- **False Data Injection**
- **DNS Hijacking**

REFERENCES

[1] https://safetyculture.com/topics/risk-assessment/5x5-risk-matrix/

[2] https://www.shodan.io/search?query=inverter

[3]

ACKNOWLEGEMENTS

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.