Substation Cybersecurity Architectural Design

Pingal Sapkota

Graduate Student

Michigan Technological University

galvin center for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society®

Outline

- Introduction
- Background
- System Model
- Substation Communication Architecture
- Design Prototypes
- Conclusion

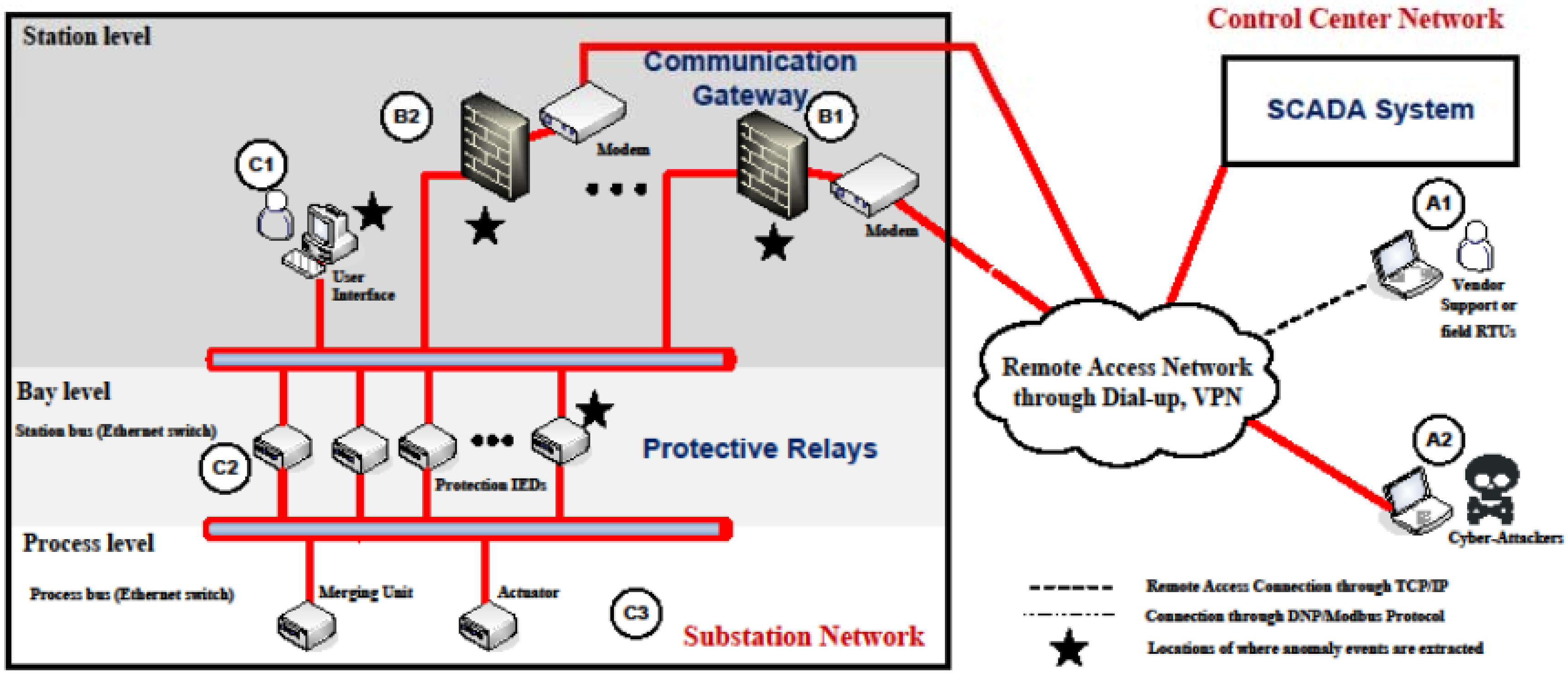
Introduction

- IP based communication infrastructure
- Exposure to unauthorized users
- Boundary protection mechanism
- Unidirectional communication gateway

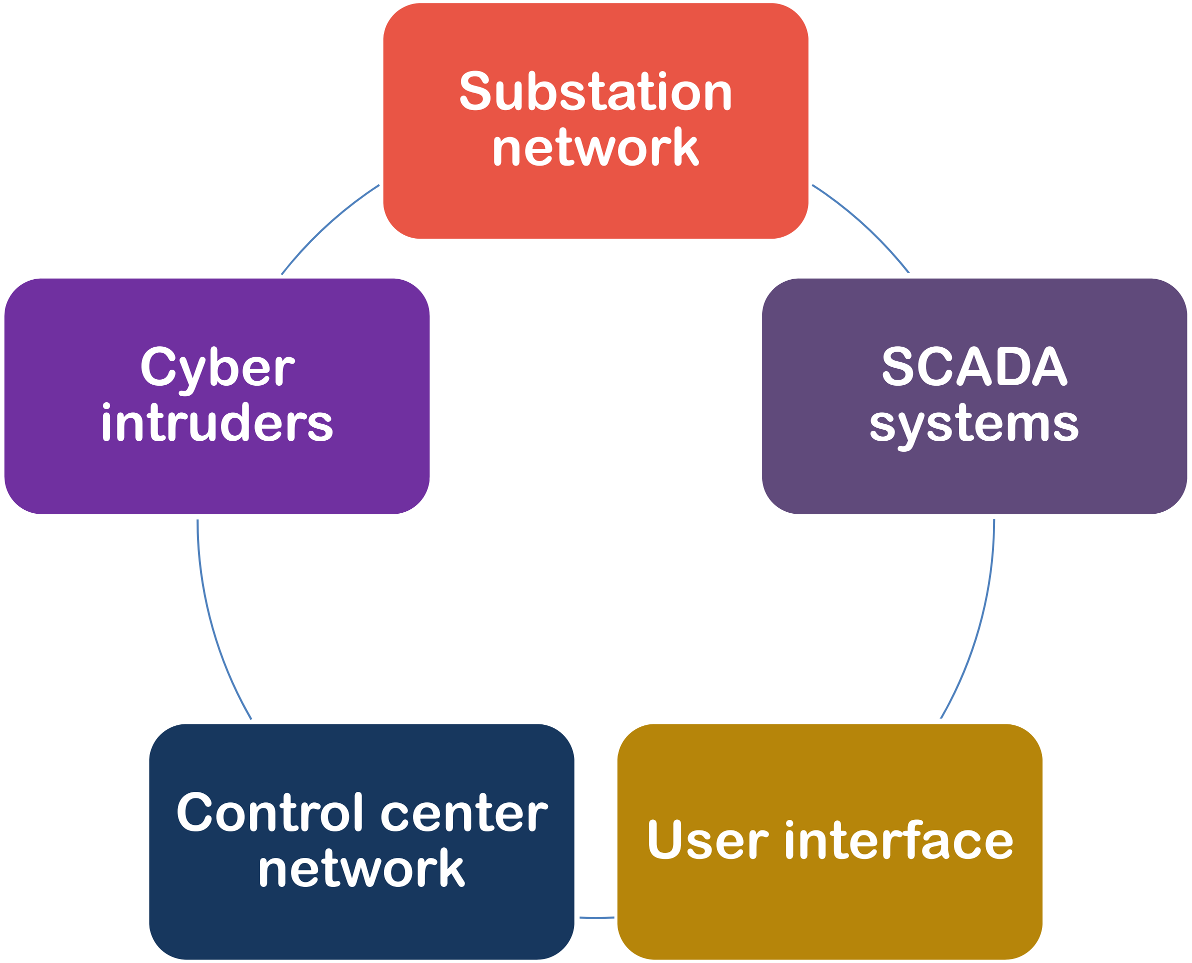
Background

- Firewalls are not designed to protect the critical infrastructure of the power system
- Performance of firewalls depend upon strategic planning and management
- One-way communication can limit the flow of data packets in only one direction
- Data diodes can physically restrict the data flow in the network
  - “The Pump”
  - “Waterfall one way”

System Model


Station level
Communication Gateway
B2
B1
C1
Modem
Modem
User Interface
Bay level
Station bus (Ethernet switch)
C2
Protective Relays
Protection IEDs
Process level
Process bus (Ethernet switch)
Merging Unit
Actuator
C3
Substation Network
Control Center Network
SCADA System
A1
Vendor Support or field RTUs
Remote Access Network through Dial-up, VPN
A2
Cyber-Attackers
Remote Access Connection through TCP/IP
Connection through DNP/Modbus Protocol
Locations of where anomaly events are extracted

System Model



Substation Communication Architecture

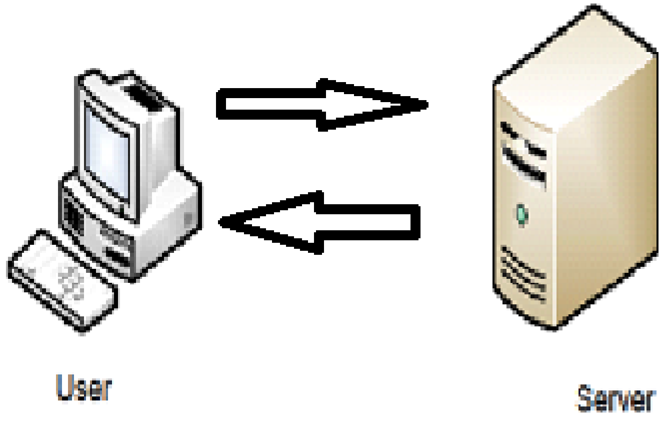
How an attack works?

1. Gain access to the communication network through the access points

2. Gather as much information

3. Understand the process

4. Gain control of the process



Substation Communication Architecture

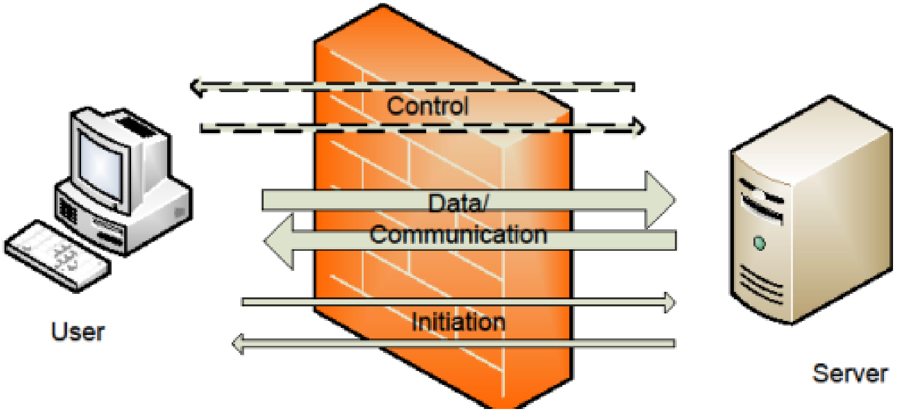
Bidirectional communication

- Communication is initiated by the external host

- Acknowledgement of the successful communication is received

- Data packets are sent through the firewall

- Intruder can mask the malicious data pretending it to be originated from an authorized source



Substation Communication Architecture

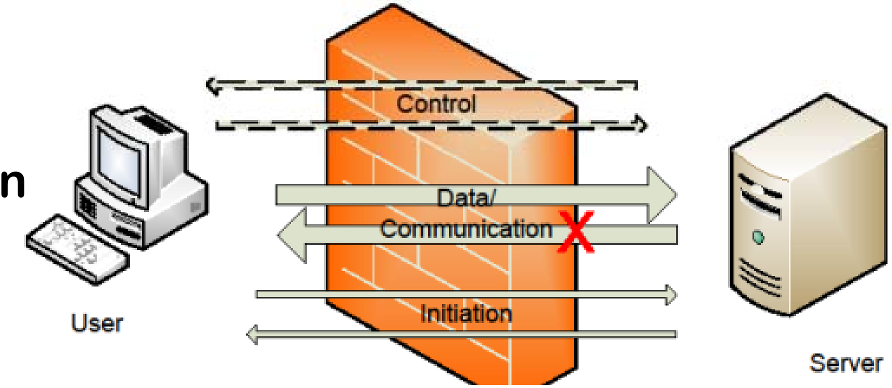
Partial unidirectional communication

- Flow of data can take place in only one direction

- No data backflow is allowed

- One-way communication can have different levels of enforcements

- Communication in the reverse direction is still possible

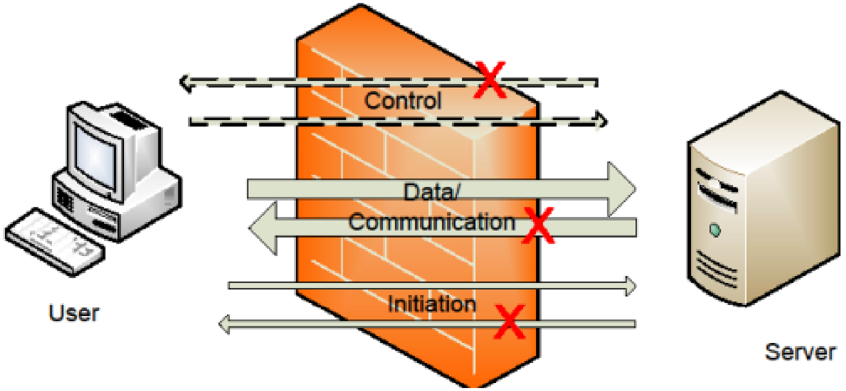


Substation Communication Architecture

Complete unidirectional communication

- Communication is strictly one way

- Information flow in the reverse direction is not possible



Two layers of unidirectional communication

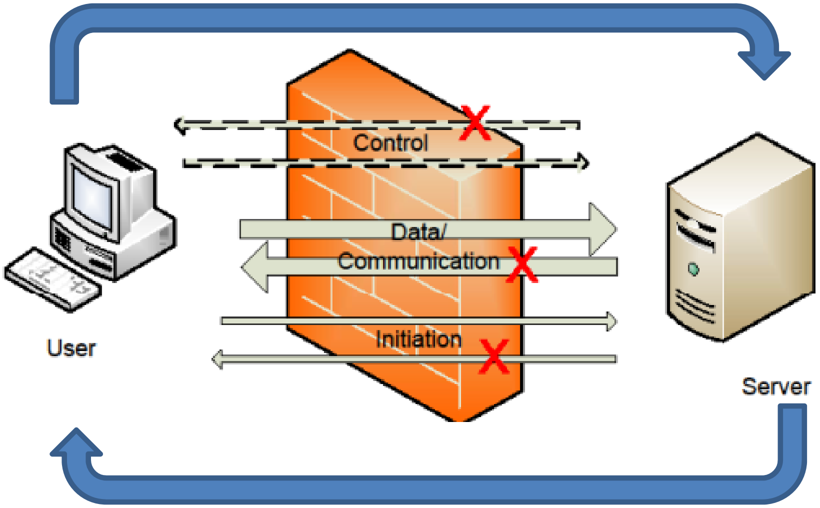
- It can improve the level of enforcement

- Data has to pass through two layer of filters instead of one

Substation Communication Architecture

Alternative communication pathways

- Virtual private network (VPN)
- Remote terminal unit (RTU)
- Field workers
- Direct connection to the modem

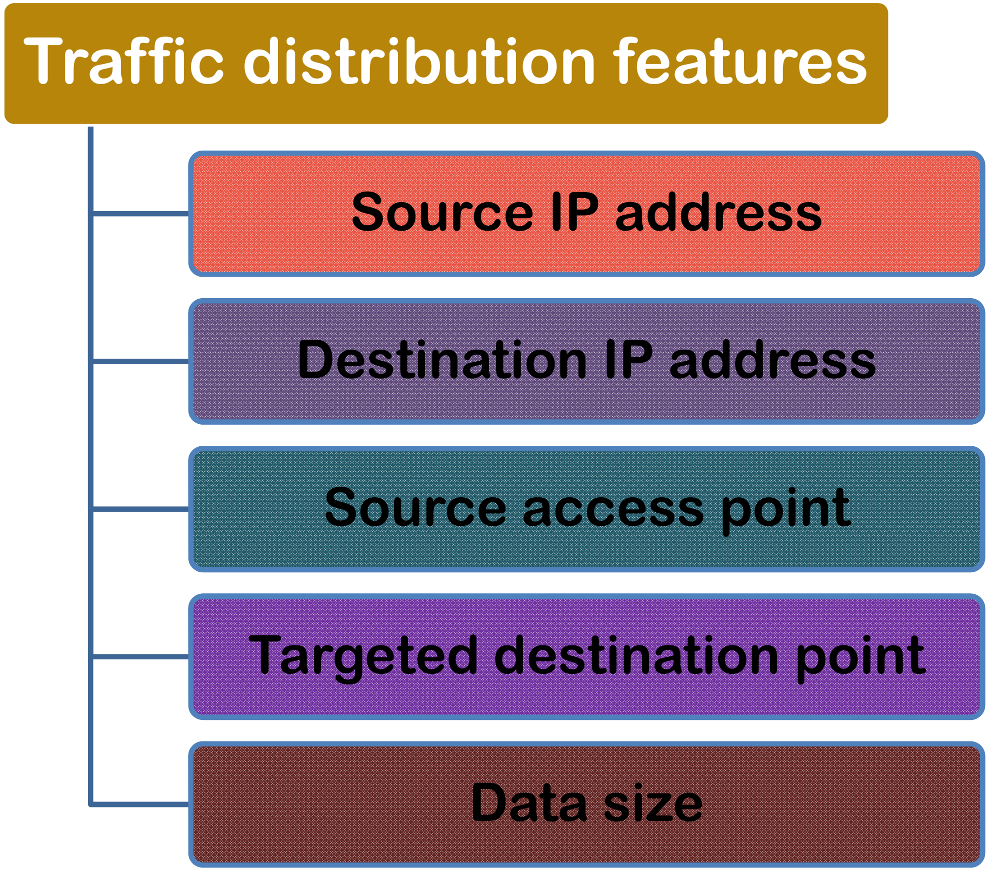


Boundary protection within a substation

1. One-way communication is not designed to replace the boundary protection and other protection technologies that are used within the substation

2. Anti-virus software help in maintaining system integrity

Design Prototypes



Traffic distribution features

- Source IP address
- Destination IP address
- Source access point
- Targeted destination point
- Data size

•These features should be evaluated in a quantitative way to determine the vulnerability of the network

•Degree of vulnerability depend upon successful data packets that reach the targeted destination within minimum trials or in shortest time

Cybersecurity features

Time to access

Connection establishment

Number of successful intrusions

Total number of attempts

Volume of data flow

Spreading malicious packets

- Longer it takes for the communication to establish, longer it takes to launch an successful attack

- In a complete unidirectional communication, attackers will have no knowledge regarding the success of their intrusion attempt

- A successful connection of the attacker with the internal host is considered a successful attack

Conclusion

- Cyber attacks in the substation infrastructure are real
- Defense mechanism is required
- Critical infrastructure needs to be protected
- Unidirectional communication is a useful alternative
- Future work and possible challenges
  - Quantifying key features of the new architecture
  - Maintaining reliability and performance of the network

References

[1] L. Pietre-Cambacedes, M. Tritschler, and G. Ericsson, “Cybersecurity myths on power control systems: 21 misconceptions and false beliefs,” Power Delivery, IEEE Transactions on, vol. 26, no. 1, pp. 161 –172, jan. 2011.

[2] X. Yue, W. Chen, and Y. Wang, “The research of firewall technology in computer network security,” in Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on, vol. 2, nov. 2009, pp. 421 –424.

[3] R. Zalenski, “Firewall technologies,” Potentials, IEEE, vol. 21, no. 1, pp. 24 –29, feb/mar 2002.

[4] M. H. Kang, I. S. Moskowitz, and S. Chincheck, “The pump: A decade of covert fun,” Computer Security Applications Conference, Annual, vol. 0, pp. 352–360, 2005.

[5] H. Okhravi and F. T. Sheldon, “Data diodes in support of trustworthy cyber infrastructure,” in Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, ser. CSIIRW ’10. New York, NY, USA: ACM, 2010, pp. 23:1–23:4. [Online].

Available: http://doi.acm.org/10.1145/1852666.1852692