NREL Transforming ENERGY

2023 ASHRAE Annual Conference

A Cybersecurity Testbed for Smart Buildings

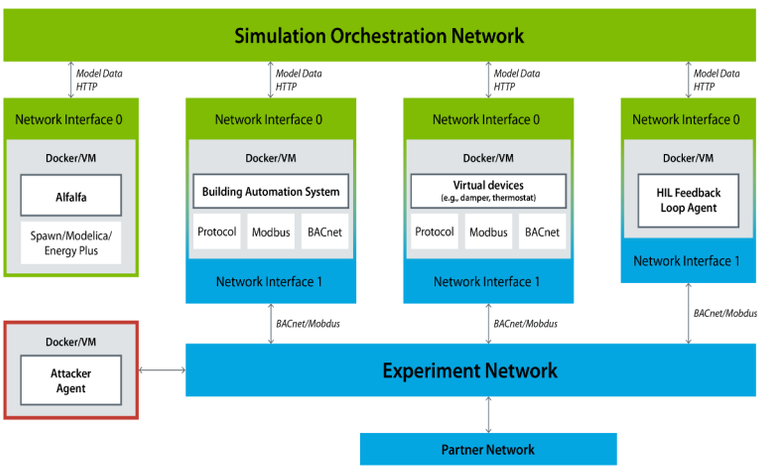
Sivasathya Balamurugan, Steve Granda, Selam Haile, Anya Peterson, Jing Wang, Jiazhen Ling
National Renewable Energy Laboratory
Acknowledgment: University of Central Florida, University of Massachusetts Lowell and Siemens

OBJECTIVES

- Smart buildings have both legacy devices and communication protocols that were not designed for secure cyber connections to operational technology networks, so they are susceptible to cyberattacks.
- With increasing cyber threats in recent years, smart buildings have become an increasing target for attacks, but not enough published data are available from these incidents to study or replicate the scenarios to defend buildings.
- So, we have created a testbed for smart buildings that can help understand the impacts of cyber-attacks on buildings by generating both physical and cyber data for analysis and evaluate cyberattack detection tools in a secure environment.

APPROACH

- This test bed includes a virtual building, virtual devices, emulated operational technology networks, and remote hardware-in-the-loop.
- Buildings research tools doesn't generally emulate networks but it's essential for cybersecurity research, thus a unique feature of the testbed.
- The malicious actor is another virtual device used to attack building devices communicating over the experiment network.
- The attacker device is configured to perform attacks on specific points by manipulating the communication through methods such as denial of service and register flooding



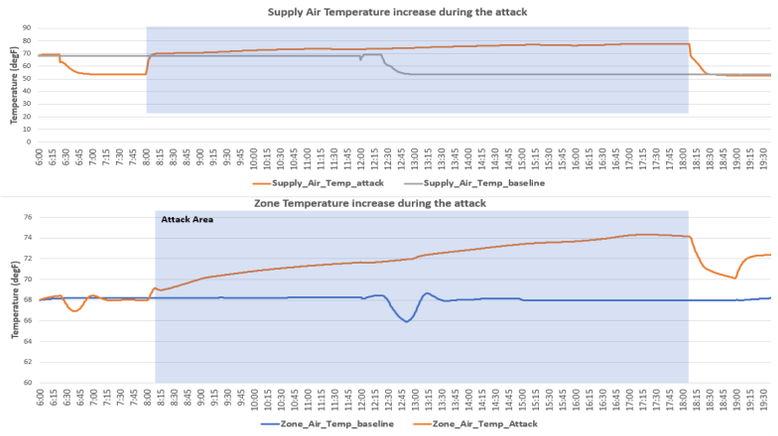
Architecture of cybersecurity testbed

EXPERIMENTAL SCENARIOS

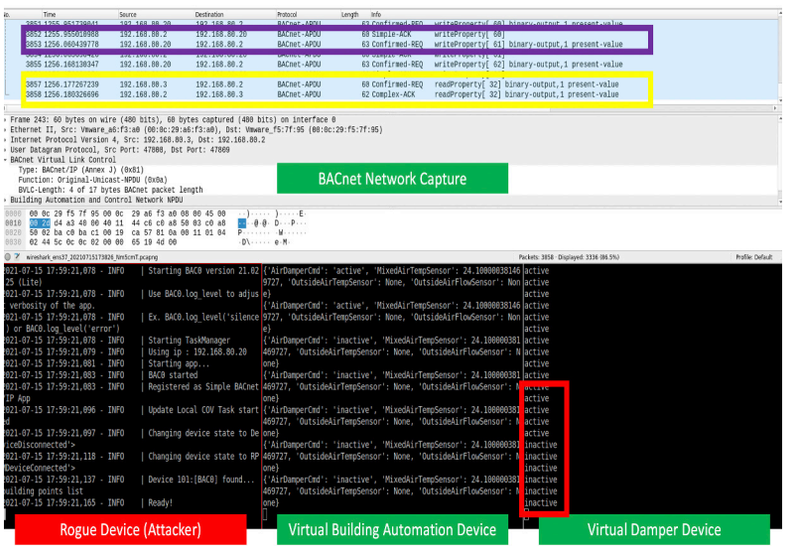
Building Model	Season	Cyber-Induced Fault	Impact
Medium office	Summer	Cooling coil stuck closed	Thermal discomfort
Medium office	Winter	Simultaneous heating and cooling	Energy waste, increased operational cost
Medium office	Winter	Outside air damper stuck open	Energy waste
Campus	Summer	Overridden thermostat set point	Occupant discomfort and energy waste

RESULTS

- During normal operation, the cooling coil valves are controlled by the supply air temperature set point, whereas the VAV dampers are controlled by the space temperature set points.
- During an attack, the operation of the cooling coil was disrupted by commanding it to be stuck closed.
- This increase would cause thermal discomfort or affect processes or equipment in spaces such as a data center.



"Cooling coil stuck closed" attack on a multizone VAV system in a medium-sized office



Wireshark network capture of cyberattack under progress

CONCLUSION

- The test bed replicates and simulates the building using Alfalfa with a defined building model to study the impacts of cyberattacks with the least impacts on real buildings and occupants
- To prevent potential cyberattacks on buildings, it is important to identify their vulnerabilities and take measures to improve them.
- Vulnerability analyses, attack detection, and mitigation systems that have the least impact on occupants and the buildings are needed, which can be enabled or evaluated using the testbed

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Buildings Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

ASHRAE Annual Conference
Tampa, Florida
June 24-28, 2023
NREL/PO-5R00-86474