GATE: Integrating Agentic AI Stack into Cyber-Physical Systems

Doguhan Yeke†, Tianle Yu‡, Matthew Lau§, Noah Spahn‡, Wenke Lee§, Giovanni Vigna‡, Dongyan Xu†, and Z. Berkay Celik†

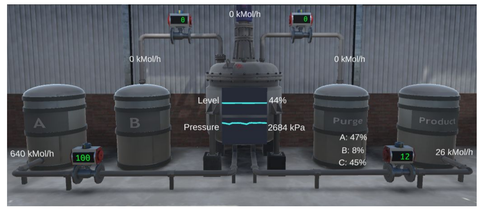
†Purdue University ‡University of California Santa Barbara §Georgia Institute of Technology

Introduction

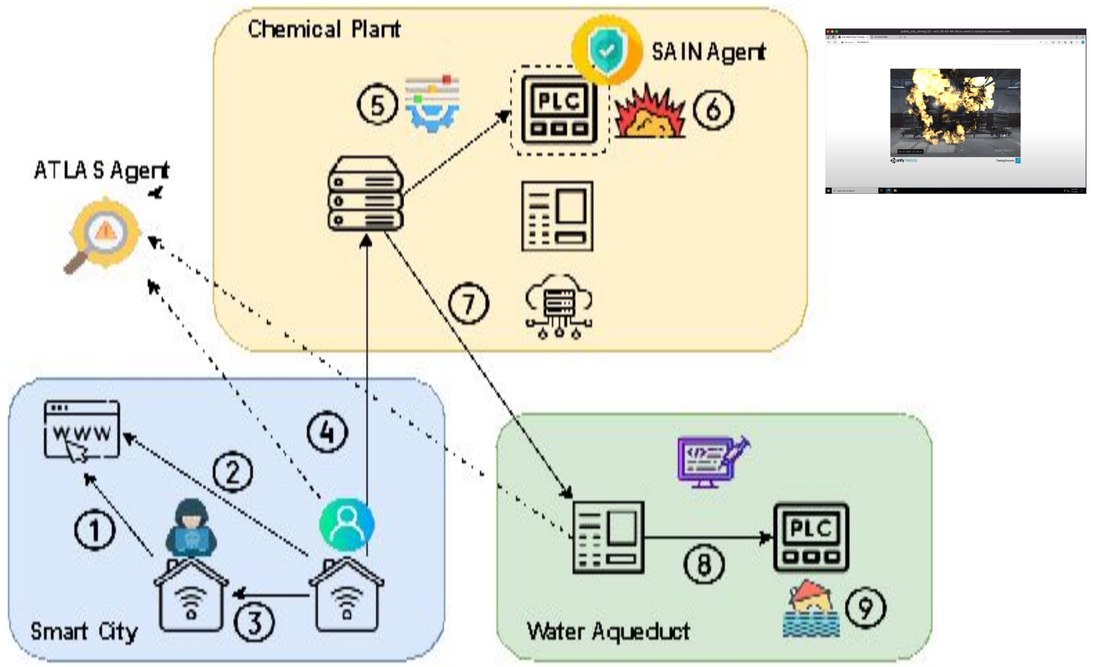
GATE provides an AWS-based testing platform to run large-scale and comprehensive experiments to evaluate all facets of the Institute's research in realistic settings.

GATE includes three main components:

1. **Smart City** includes Linux-based machines that the users in smart homes
2. **Las Palomas Power Plant** involves two feed supplies given to the reactor for an exothermic reaction
3. **Great Aqueduct** runs a water treatment plant simulator that purifies raw water through several PLC-controlled processes

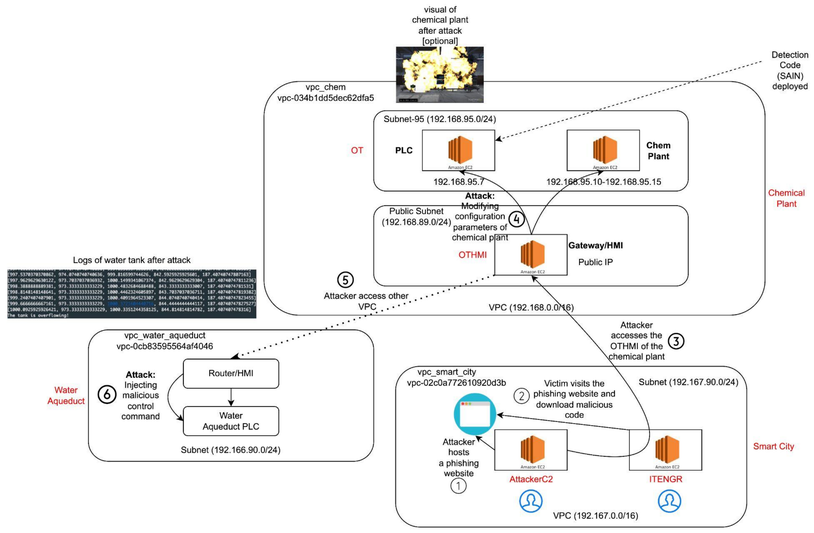


Attack Overview



1) Attacker serves a phishing website
2) Victim downloads and runs payload
3) Attacker exfiltrates important ICS schematics
4) Laterally moves to power plant HMI
5) Modifies the PLC configuration parameters
6) The power plant explodes
7) Laterally moves to great aqueduct
8) Injects malicious actuator command
9) The water tank overflows

AWS Overview



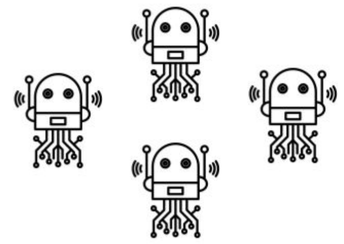
SAIN [1] is an **attack detection and mitigation agent** that generates and enforces state-aware knowledge with tight PLC variable value bounds to protect industrial control systems.

ATLAS [2] is an **attack investigation agent** that integrates natural language processing and deep learning techniques into data provenance analysis to model sequence-based attack and non-attack behavior.

Ongoing Agent Deployments

Integrating more agents including:

- Correlation agent
- Sharing agent
- Human agent interaction
- Filesystem
- Network



References

[1] Syed Ghazanfar Abbas, Muslum Ozgur Ozmen, Abdulellah Alsaheel, Arslan Khan, Z. Berkay Celik, and Dongyan Xu. SAIN: Improving ICS Attack Detection Sensitivity via State-Aware Invariants. Usenix Security 2024.

[2] Alsaheel, Abdulellah, Yuhong Nan, Shiqing Ma, Le Yu, Gregory Walkup, Z. Berkay Celik, Xiangyu Zhang, and Dongyan Xu. ATLAS: A sequence-based learning approach for attack investigation. USENIX Security 2021.

AI Institute for Agent-based Cyber Threat Intelligence and Operation

Supported by the National Science Foundation under grant no. IIS-2229876 and is supported in part by funds provided by the NSF, by the Department of Homeland Security, and by IBM.

https://action.ucsb.edu