Using Machine Learning to Monitor Remote Connection Sessions

ELECOMP Capstone Design Project 2024-2025

Sponsoring Company:

Dispel LLC
61 Greenpoint Ave, Suite 634,
Brooklyn, NY, 11222, US
https://dispel.com

Company Overview:

Founded in 2014 and headquartered in Austin Texas, Dispel is a leading provider of zero trust access and moving target defense for cyber physical systems. Our all-in-one remote access and data streaming platform makes it easy to manage, control, and audit operators and third-parties who need access to your industrial control systems. Quick to implement and easy to use, Dispel simplifies industrial control system modernization by combining cybersecurity frameworks and regulatory compliance with streamlined features for real-time operations. Every day, millions of people depend on us in water, defense, automotive, manufacturing, energy, and extraction. We can't wait to show you how your operations can be safer and easier too

Technical Director:

Constantine (Dean) Macris
Chief Information Security Officer
dean.macris@dispel.com
https://www.linkedin.com/in/constantine-macris-4ab26310/

Project Motivation:

Dispel provides secure remote access for customers to various critical infrastructure networks. The Dispel Zerotrust Engine for Remote Access (DZTE-RA) instantiates a compostable workstation (Virtual Desktop) for engineers to maintain or service programmable logic controllers (PLCs) or access other engineering workstations inside the environment. The DZTE-RA provides a feature of screen recording that enables an administrator to review or even watch the actions any engineer is accomplishing in the environment. For larger systems, administrators can't watch or even review all screen recordings unless there is some event that triggers review (an incident or mistake was made).

Dispel is interested in designing a system that can categorize different types of user actions through screen recordings. These actions are classified based on administrator-designed rules. The end goal is to enable an anomaly in the engineer's action (using the wrong program or running unauthorized commands) to trigger an alert and disconnect the system from the network.

The project will include developing the software and machine learning mechanisms for various windowed applications, developing a method to determine text commands from screen recordings, implementing it into the current web application stack, and designing the infrastructure to deploy and test the application.

The capstone team will be working with the Dispel Product Team and Engineering Team to design an MVP for the system, lay out a roadmap to integrate it into the current platform, and possibly roll out the feature in the DZTE-RA product while getting experience working in a cybersecurity technology SaaS company.

Anticipated Best Outcome:

- Develop models to categorize 50% of customer applications
- Method for training additional applications, designed into platform
- Ability to pull text commands from the screen recordings
- Integration of an aspect of the project into the current DZTE-RA software stack
- Student integration into Dispel engineering team

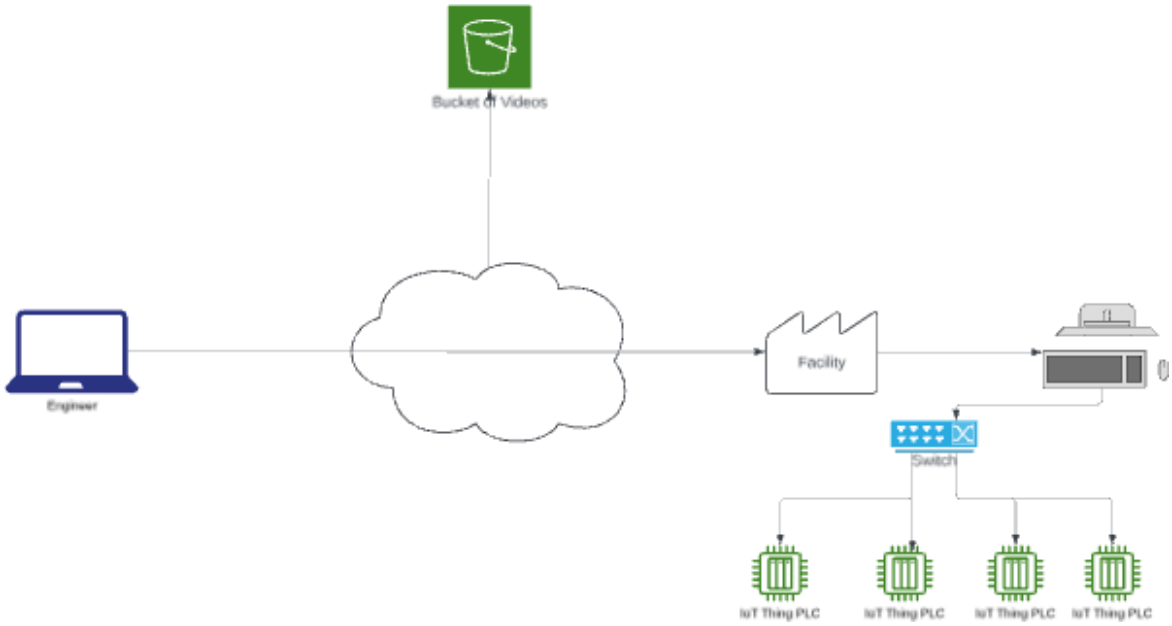
Project Details:

The purpose of this capstone project is to use machine learning to develop a system to categorize different types of behavior in recordings of remote desktop sessions, and then allow the system to categorize a given behavior as authorized or unauthorized against either pre-set conditions or an average baseline.

Dispel has hundreds of hours of screen recordings that contain approved workflows for plant engineers. The project will utilize these recordings to first develop a supervised training model to categorize applications engineers use and prove that the model can be utilized to categorize the applications through screen recordings as an engineer is operating. The second feature will be the ability to gain context into the commands being run through OCR and utilize LLM to categorize the text commands on-screen. The project will work with Dispel security professionals to develop approved and unapproved commands to categorize around.

The academic proof of concept will then need to be integrated into a proof of concept in the DZTE-RA web stack where the project will become integrated into the Dispel software development lifecycle and additional features needed to make the idea into a product will be developed, spiked, scoped and completed by the project team in conjunction with the Dispel Engineering/Product team.

Finally, the outcome of giving customer administrators the ability to identify approved and unapproved applications and commands from inside the DZTE-RA tool is the ultimate goal. There are various levels of success from being implemented as a “Pull Request” (waiting for the right time to merge into the main line software project) to a Development Release to a full Production Release.



Composition of Team:

2 Computer Engineers **(preference will be given to those taking the course with Megan Chiovaro on Thursday evenings)**

Skills Required:

Computer Engineering Skills Required:

- Python
- Machine Learning
- Full Stack (NodeJS, TypeScript)

Anticipated Best Outcome's Impact on Company's Business, and Economic Impact

Dispel is hoping to be able to take the work done in this project and utilize it to provide a first- of-its-kind system to protect critical infrastructure from obscuring activity through the Dispel tool by utilizing "jump hosts".

DISPEL
Remote Access Systems