Analyzing Airplane System and Security Logs for Context Awareness

STUDENTS: ZIYANG GONG, ZIMU LI, NAM NGUYEN, STEVE SU, CHENGZHI XU, JIAMING ZHANG

INTRODUCTION

- The cybersecurity team at Boeing has tasked the UW ENGINE team to develop a cybersecurity threat detection, identification, and mitigation algorithm to assist engineers and airline personnel in dealing with cybersecurity threats.
- The UW ENGINE team was also tasked with researching and designing an embedded device to generate log files on aircraft devices to normalize and generate log files for devices that are not utilizing Boeing's standards.

TECHNOLOGY STACK and TOOLS

- Developed the backend using Flask and leveraged Echarts for interactive data visualization on the front-end
- Implemented Firebase as the database solution for handling user authentication.
- Developed a Flask Cache mechanism aimed at enhancing the browsing speed of voluminous log files.
- Utilized Pandas to preprocess raw log files and applied clustering algorithms from scikit-learn for log analysis purposes.

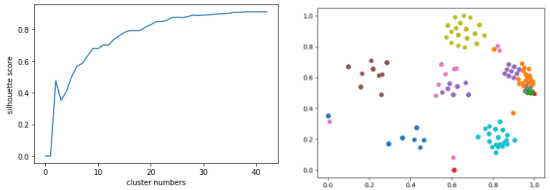
USE CASES

Use Case 2: Cyber Event Response and Mitigation
- Log Data Analysis Algorithm Design, Log Anomaly Response Design, Analyzed Data Results Visualization. (Algorithm Design)
- Draft User Interface, Functions Regards the Algorithm, Optimize Presentation Methods (Webpage Creation)

Use Case 1: Security Event Classification
- Aircraft Control Domain
- Airline Information Services Domain
- Passenger Information and Entertainment Services Domain

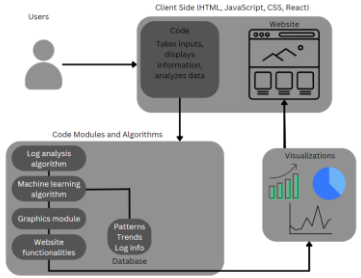
IMPLEMENTATION

Back-End:
- Gaussian Mixture Model is used to group episodes into different groups
- Silhouette score is used to get the best clustering numbers for different datasets.



- The API utilizes Ajax requests to processing asynchronous requests.
- The API supports the following HTTP requests:
- GET -POST -PUT -DELETE
- NPM is utilized for automatic installation of dependencies and for running the backend script upon deployment to the server using the GitHub pipeline.
- Enhanced the clustering algorithm to efficiently handle various log file formats and types.

Front-End:
- Designed different pages for different datasets (dataload, firewall, staging)
- Implemented interactive charts using JavaScript
- Implemented user login function with user email verification for security
- Optimized backend analysis for efficient website performance



FUTURE DEVELOPMENT

- The website will need further improvements on portability and overall usability, with an emphasis on data interaction and design.
- Adding more information that can be useful in threat mitigation as well as possible solutions can further improve website function and use.
- Additional research as well as the design, implementation, and prototyping of the embedded device will also need to be done to satisfy Boeing's needs.

CONCLUSION

In conclusion, the project has been a significant milestone in enhancing the security and protection of aircraft systems. Through the implementation of advanced log analysis algorithms and machine learning techniques, we have successfully built an automated process that detects cybersecurity events in real-time. Working closely with industry professionals from Boeing and receiving guidance from our academic advisors, we have gained valuable insights into the practical challenges and considerations in the field of aircraft cybersecurity. Our project findings and results have been well-received, demonstrating the effectiveness and value of our automated cybersecurity event detection system.

ACKNOWLEDGMENTS, and REFERENCES

We would like to express our sincere gratitude to Dave Mier, Emily Zhang, and Rafka Daou from Boeing as well as our faculty advisor Dinuka Sahabandu and our TA, Harsha Vardhan.

[1] *Documentation - Apache ECharts*. Documentation - apache echarts. (n.d.).
[2] Editor, C. C. (n.d.). *Cybersecurity event - glossary: CSRC*. CSRC Content Editor.
[3] Google. (n.d.). *Firebase documentation*. Google.
[4] *Welcome to flask¶*. Welcome to Flask - Flask Documentation (2.3.x). (n.d.).

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

TECHNICAL ADVISORS: DAVID MIER, JOSEPH MCGOOGAN-JR, EMILY ZHANG, RAFKA DAOU
FACULTY ADVISORS: Dinuka Sahabandu, Harsha Vardhan
SPONSORS: BOEING