COVID-19 Android Malware Detection Using Permissions and App Icons

By: David Tan
Mentor: Alfredo J. Perez
TSYS School of Computer Science

Presentation Overview

Problem Statement

Introduction

Methodology

Results

Conclusion

Future Work

Problem Statement

Since the start of the COVID-19 pandemic in late 2019, there has been a dramatic increase in the percentage of malicious applications targeting mobile devices worldwide which indicates that malicious developers are capitalizing on the COVID-19 pandemic. The popularity and the ease of Android mobile application distribution have further spurred the interest of many cyber-criminals across the globe. Disguised as benign applications, these malware applications are taking advantage of the asymmetry between irrelevant/redundant permissions and informative permissions of benign Android applications in order to access the sensitive and private information on these devices.

Introduction: Background

As the use of systems, applications, and software is on the rise globally, user privacy and data protection are of the utmost concern to individuals, firms, and businesses operating online. Furthermore, there has been a significant increase in the number of Android malware applications since the start of the COVID-19 pandemic. Android's status as one of most commonly used smartphone operating systems and its daily increase in applications in the smartphone application market has made the scope of this issue of increasingly emerging Android malware applications a pressing issue in the industry. These malicious Android applications, disguised as benign applications, are designed to either steal users' private information or make profit by phishing and extortion in the form of malware like worms, exploits, Trojans, and viruses.

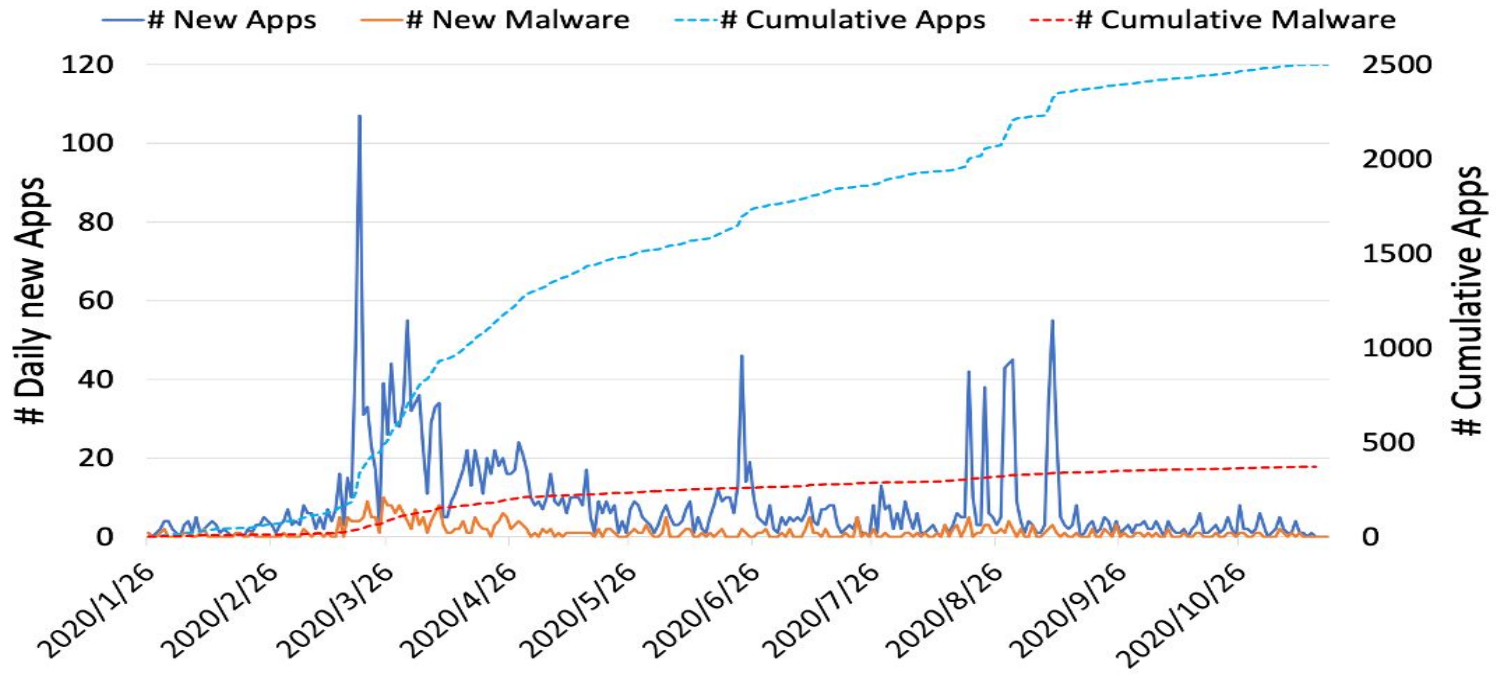


Fig. 2: Number of COVID-19 related apps and malware over the time (from Jan to Nov 2020).

Introduction: Our Research

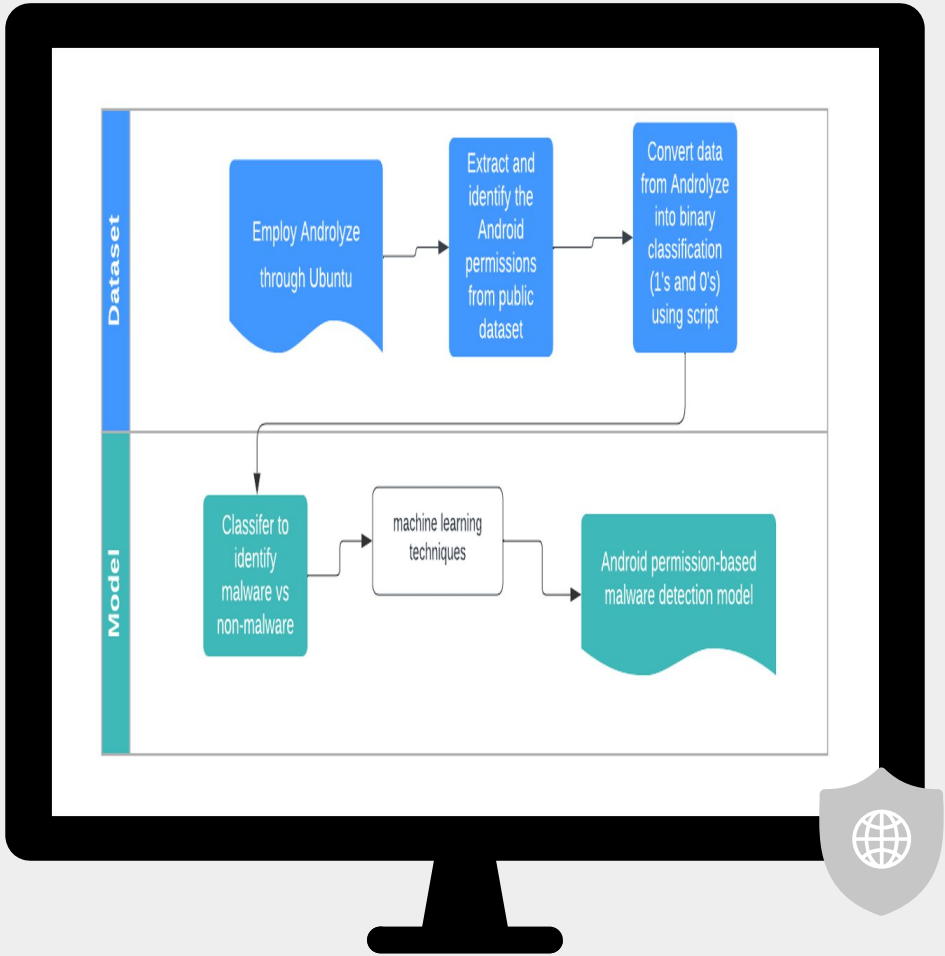
In this paper, we propose an Android permissions-based COVID-19 malware detection system that determines if an application is malicious based on the usage of suspicious permissions. The system used a multi-level based methodology. First, we extracted and identified the Android permissions and icons from the public dataset of 2,017 applications of the research paper “Beyond the virus: A First Look at Coronavirus-themed Android Malware” by employing the python tool Androguard. We then utilize a machine learning model to categorize the applications as either malware or non-malware based on the usage of suspicious permissions.

Methodology: Concept

The system used a multi-level based methodology. First, we extracted and identified the Android permissions and icons from the public dataset of 2,017 applications of the research paper “Beyond the virus: A First Look at Coronavirus-themed Android Malware” by employing the python tool Androguard. We then utilize a machine learning model to categorize the applications as either malware or non-malware based on the usage of suspicious permissions. Through extensive experiments, the proposed model has demonstrated a high level of symmetry between irrelevant permissions and malware applications. We tested the accuracy of the proposed model through extensive experiments in order to see if it possessed a high level of symmetry between irrelevant permissions and malware applications.

Methodology: Overview

Fig. 1. shows an overview of our multi-level-based methodology to produce our Android permission-based malware model.

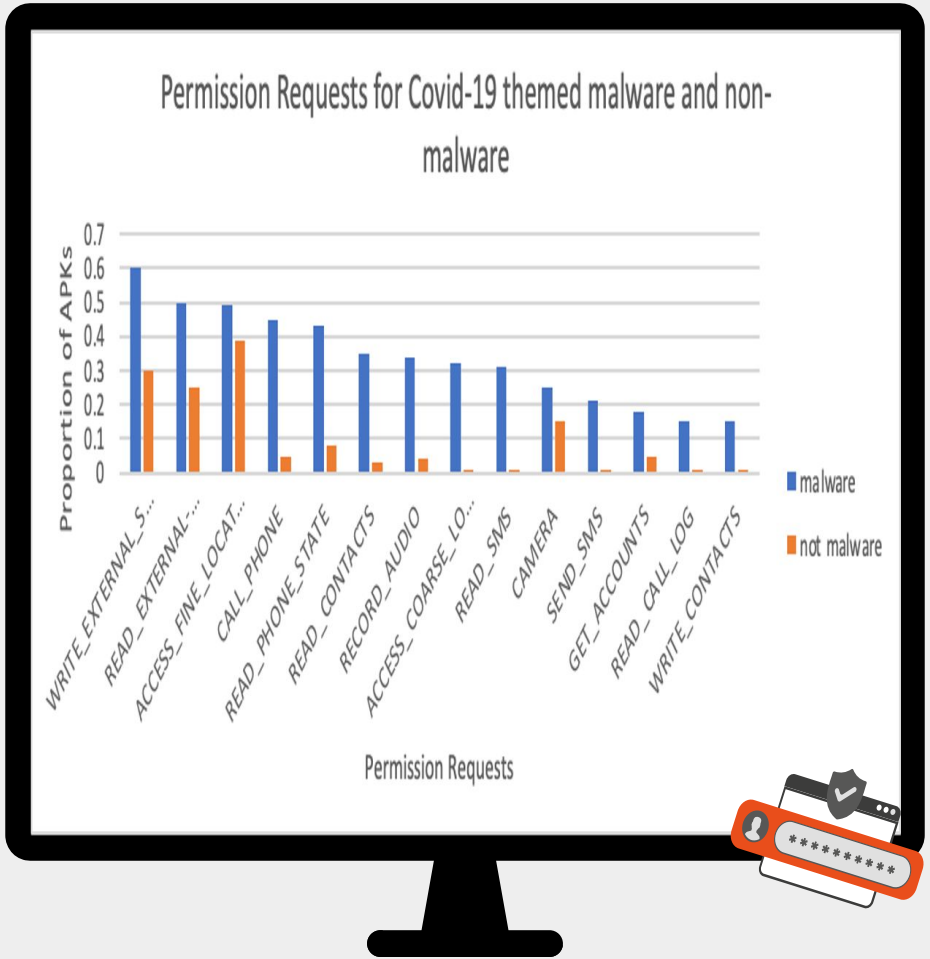


Methodology: Androguard

Fig. 2. “Permission Requests for COVID-19 themed malware and non-malware” presented similar results to those found in the paper “Beyond the Virus: A First Look at Coronavirus-themed Android Malware” which serves to validate our research and methodology.

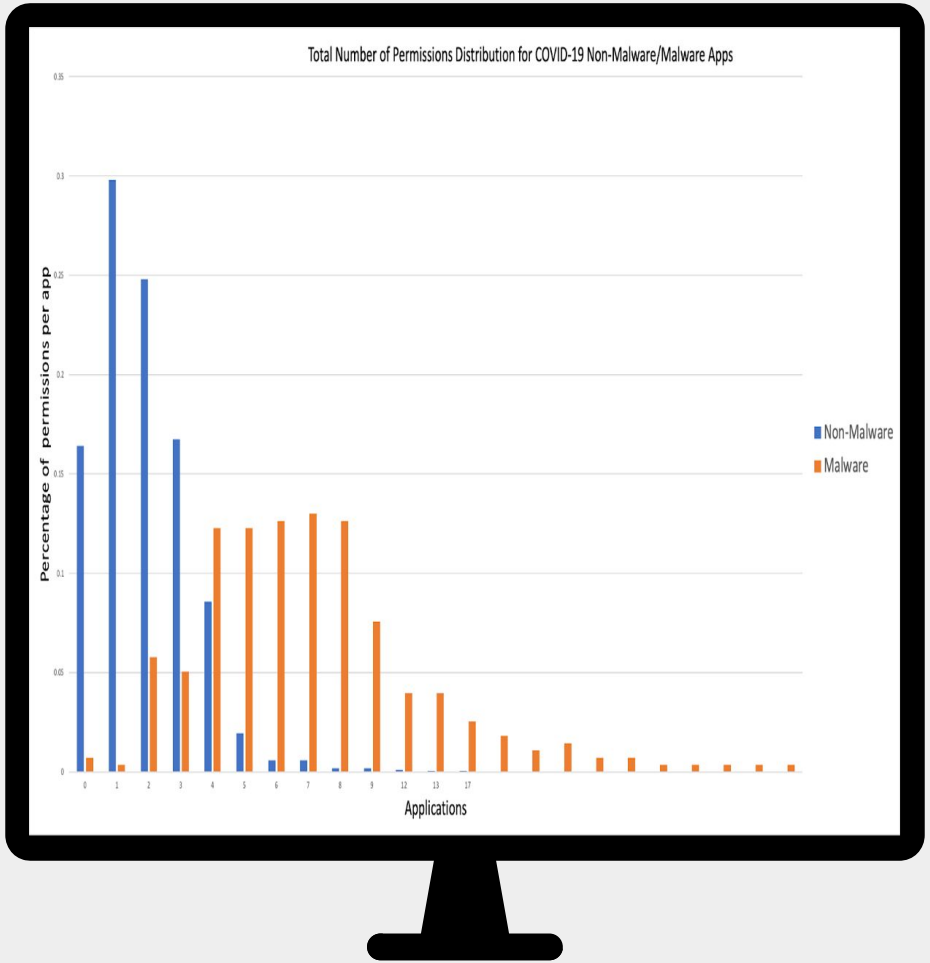
Results: Permission Requests

Fig. 3. “Permission Requests for COVID-19 themed malware and non-malware” presented similar results to those found in the paper “Beyond the Virus: A First Look at Coronavirus-themed Android Malware” which serves to validate our research and methodology.



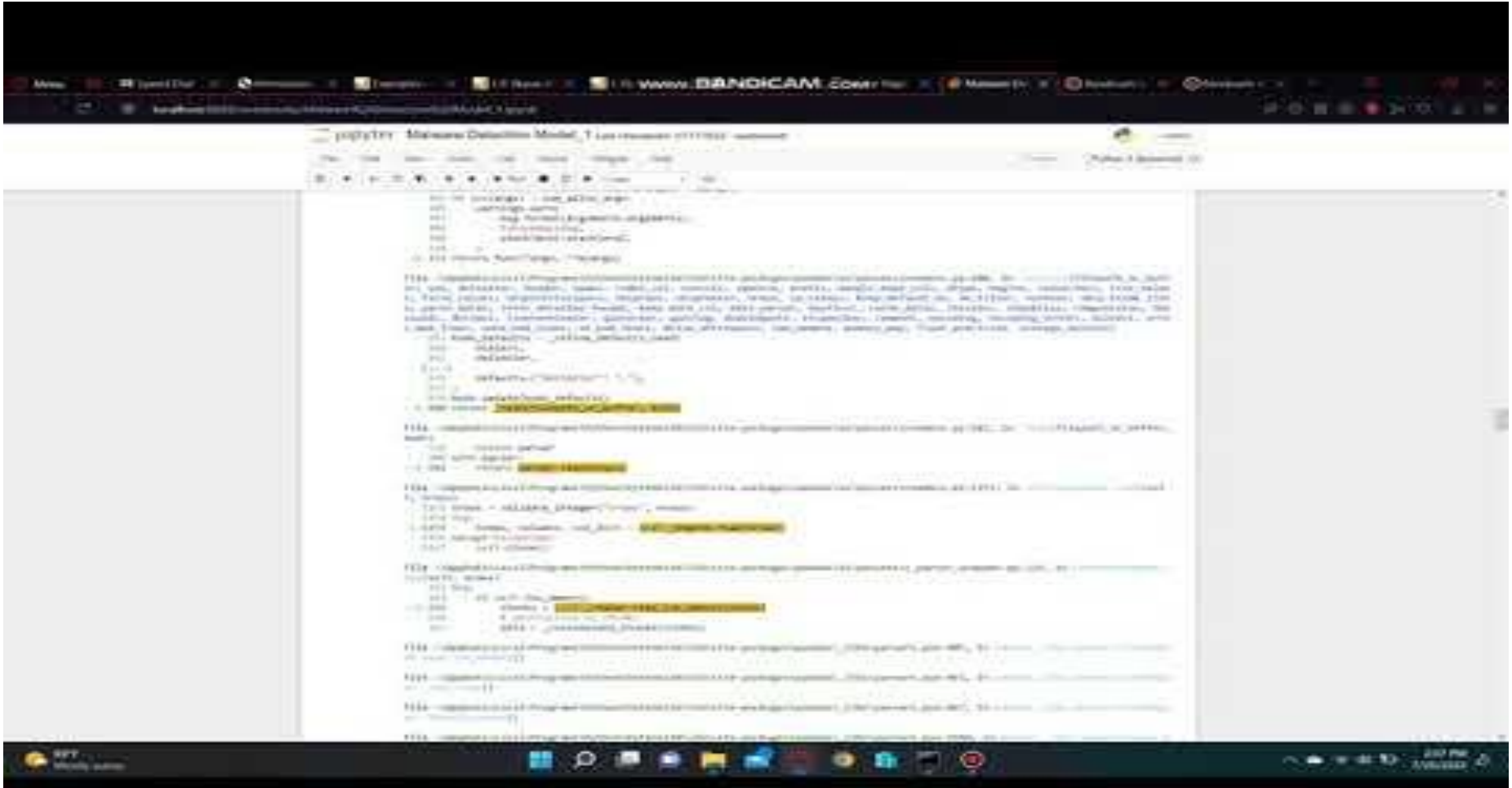
Results: Permission Distribution

Fig. 4. “Total Number of Permissions Distribution for COVID-19 Non-Malware/Malware Apps” served the purpose of confirming the feasibility of our research goal to create an Android permissions-based COVID-19 malware detection system with machine learning technologies.



Model 1

Android permissions-based COVID-19 malware detection system that determines if an application is malicious based on the usage of suspicious permissions.



Conclusion

In conclusion, the popularity and the ease of mobile application distribution have spurred the interest of many cyber-criminals across the globe. This interest has been further fueled by the COVID-19 pandemic, and since its start, there has been a dramatic increase in the percentage of malicious applications targeting mobile devices worldwide. With the purpose of providing an alternative for Android malware detection for malicious applications, we have proposed an Android permissions-based COVID-19 malware detection system. Through extensive experiments, the proposed model has demonstrated a high level of symmetry between irrelevant permissions and malware applications. The proposed system has the potential to provide a low-cost alternative for Android malware detection for malicious applications including repacked applications.

Future Work

Due to the time constraint associated with a summer undergraduate research, we were not able to complete our second system of an icon-based COVID-19 malware detection system. Therefore, to further our research, we would develop this model in order to complete our novel contribution to the paper “Beyond the Virus: A First Look at Coronavirus-themed Android Malware.”

References

Akbar, F., Hussain, M., Mumtaz, R., Riaz, Q., Wahab, A. W. A., & Jung, K.-H. (2022). Permissions-Based Detection of Android Malware Using Machine Learning. Symmetry (20738994), 14(4), N.PAG.

Albahar, M. A., ElSayed, M. S., & Jurcut, A. (2022). A Modified ResNeXt for Android Malware Identification and Classification. Computational Intelligence & Neuroscience, 1–20.

Almomani, I., Ahmed, M., & El-Shafai, W. (2022). Android malware analysis in a nutshell. PLoS ONE, 17(7), 1–28.

Almomani, I., Alkhayer, A., & El-Shafai, W. (2022). An Automated Vision-Based Deep Learning Model for Efficient Detection of Android Malware Attacks. IEEE Access, Access, IEEE, 10, 2700–2720

Hosseini, S., Nezhad, A. E., & Seilani, H. (2021). Android malware classification using convolutional neural network and LSTM. Journal of Computer Virology and Hacking Techniques, 17(4), 307–318.

Junyang Qiu, Jun Zhang, Wei Luo, Lei Pan, Nepal, S., & Yang Xiang. (2020). A Survey of Android Malware Detection with Deep Neural Models. ACM Computing Surveys, 53(6), 1–36.

Kim, H., Kang, M., Cho, S., & Choi, S. (2022). Efficient Deep Learning Network With Multi-Streams for Android Malware Family Classification. IEEE Access, Access, IEEE, 10, 5518–5532

Mahesh, P. C. S., & Hemalatha, S. (2022). An Efficient Android Malware Detection Using Adaptive Red Fox Optimization Based CNN. Wireless Personal Communications: An International Journal, 1–22.

Sahin, D. O., Akleylek, S., & Kilic, E. (2022). LinRegDroid: Detection of Android Malware Using Multiple Linear Regression Models-Based Classifiers. IEEE Access, Access, IEEE, 10, 14246–14259

Singh, J., Thakur, D., Gera, T., Shah, B., Abuhmed, T., & Ali, F. (2021). Classification and Analysis of Android Malware Images Using Feature Fusion Technique. IEEE Access, Access, IEEE, 9, 90102–90117

Shen, L., Feng, J., Chen, Z., Sun, Z., Liang, D., Li, H., & Wang, Y. (2022). Self-attention based convolutional-LSTM for android malware detection using network traffics grayscale image. Applied Intelligence: The International Journal of Research on Intelligent Systems for Real Life Complex Problems, 1–23.

Wang L, He R, Wang H, Xia P, Li Y, Wu L, Zhou Y, Luo X, Sui Y, Guo Y, Xu G. (2021). Beyond the virus: a first look at coronavirus-themed Android malware. *Empir Softw Eng. 26*(4):82. doi: 10.1007/s10664-021-09974-4.

Xu, J., Li, Y., Deng, R. H., & Xu, K. (2022). SDAC: A Slow-Aging Solution for Android Malware Detection Using Semantic Distance Based API Clustering. IEEE Transactions on Dependable and Secure Computing, Dependable and Secure Computing, IEEE Transactions on, IEEE Trans. Dependable and Secure Comput, 19(2), 1149–1163.

NSF

COLUMBUS STATE UNIVERSITY

Questions?