Android Malware Detection: A Hybrid Approach using Machine Learning Techniques

Presented By

Asadullah Hill Galib
MSSE 0718
Institute of Information Technology
University of Dhaka

Supervised By

Dr. B. M. Mainul Hossain
Associate Professor
Institute of Information Technology
University of Dhaka

ICT DIVISION
FUTURE IS HERE

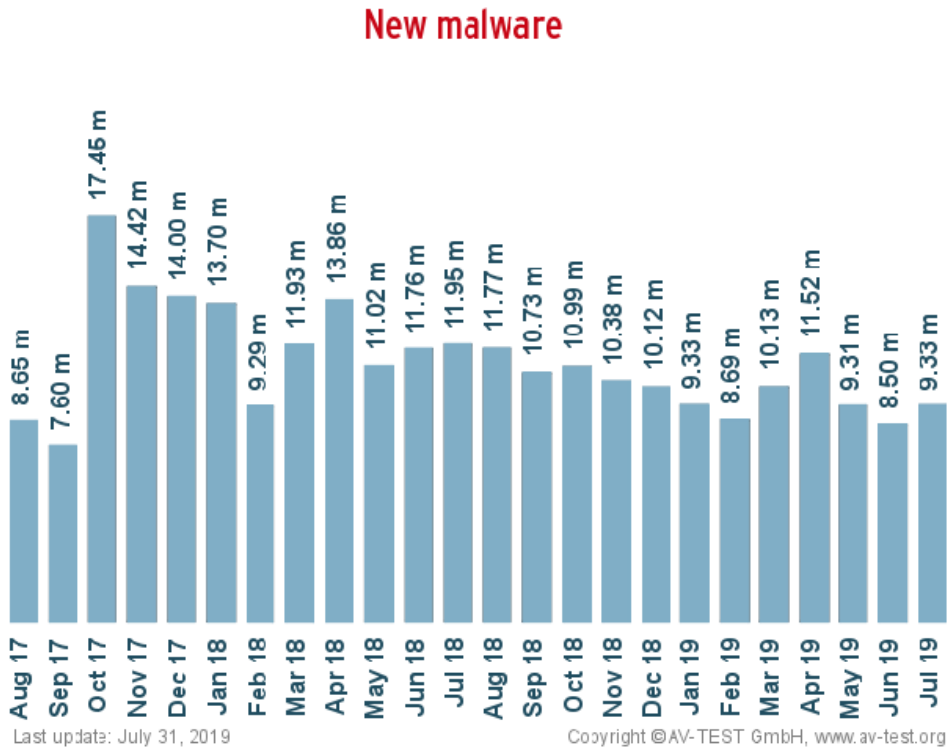
IIT
University of Dhaka

Introduction (Android Malware)

Android Malware (malicious application) is any application with mischievous intention -

- disrupt normal functioning
- bypass access controls
- gather sensitive information
- display unwanted advertising
- getting unauthorized control

Introduction (Android Malware)



Android Malware Detection Techniques

- Static Analysis
- Dynamic Analysis
- Hybrid Analysis

Drawbacks

Static Analysis	Dynamic Analysis
◎ Data obfuscation	◎ Limited code coverage
◎ Control flow obfuscation	◎ Tricked in emulated environment by smart malware
◎ Dynamic XML loading	
◎ Native code	
◎ Encryption	

Hybrid Analysis

A fusion of static and dynamic analysis would be a good candidate as it prevails over the individual drawbacks of static and dynamic analysis.

Research Question

- RQ: How can we improve the performance of android malware detection using hybrid analysis with machine learning techniques?

Research Question (sub-questions)

- SQ1. What are the important static and dynamic features for android malware detection using machine learning?
- SQ2. How to select the important static and dynamic features for android malware detection?

Rationale of the Research (Academia)

- To alleviate the evasion techniques of malware authors by integrating Hybrid Analysis.
- To improve the performance of malware detection process.

Rationale of the Research (National)

- To achieve the new millennium development goal: *Digital Bangladesh* by 2021,
  - Government has taken many projects and performed many activities regarding android app.

Rationale of the Research (National)

- This research aims to detect android malware in advance effectively.
- By so, this research work can assist the Bangladesh government's new millennium development goal - "Digital Bangladesh" by 2021.

References

- Spreitzenbarth, M., Freiling, F., Echtler, F., Schreck, T., Hoffmann, J. (2013, March).Mobile-sandbox: having a deeper look into android applications. In Proceedings of the28th Annual ACM Symposium on Applied Computing (pp. 1808-1815). ACM
- Lindorfer, M., Neugschwandtner, M., Platzer, C. (2015, July). Marvin: Efficient and comprehensive mobile app classification through static and dynamic analysis. In 2015 IEEE 39th annual computer software and applications conference (Vol. 2, pp. 422-433).IEEE.
- Arshad, S., Shah, M. A., Wahid, A., Mehmood, A., Song, H., Yu, H. (2018). Samadroid:a novel 3-level hybrid malware detection model for android operating system. IEEEAccess, 6, 4321-4339.

References

- Kapratwar, A., Di Troia, F., Stamp, M. (2017). Static and dynamic analysis of androidmalware. In ICISSP (pp. 653-662).
- Xu, L., Zhang, D., Jayasena, N., Cavazos, J. (2016, September). Hadm: Hybrid analysisfor detection of malware. In Proceedings of SAI Intelligent Systems Conference (pp. 702-724). Springer, Cham.
- OperatingSystemMarketShareBangladesh.(n.d.).Retrievedfromhttp://gs.statcounter.com/os-market-share/all/Bangladesh
- ACTIVITIES. (n.d.). Retrieved from https://www.nationalappsbd.com/?pageid= 690

Thank you!

Any questions?

ICT DIVISION
FUTURE IS HERE

IIT
University of Dhaka