컴퓨터 보안 특론
(Special Topics in Computer Security)

조성제 (Cho, Seong-je)

Spring, 2020

Computer Security & OS Lab.
Dankook University

Instructor

- 조성제 교수 (Prof. Seong-Je Cho)
  - Room 510, SW.ICT Building

    sjcho at dankook dot ac dot kr

  - Research interests: System security, SW security
  - Advisor of Computer Security & OS Lab. *(securesw.Dankook.ac.kr)*

    Dept. of Computer Science & Engineering, Dankook Univ.
  - Faculty advisor of the Aegis, Computer Security Club

  - Course Webpage
    - http://securesw.dankook.ac.kr
    - Lecture notes, Presentation schedule, etc.

Course Overview

- This course provides students
  - Current and challenging topics in the Computer Security.
  - Some technical aspects of computer security.

- During Spring 2020 semester, this course will focus on Malware Detection/Analysis
  - This research oriented class will introduce participants to interesting topics in malware detection/analysis using machine learning

- This course covers the following topics
  - The latest trends in cybersecurity
  - Reverse engineering for malware analysis
  - Signature-based malware detection
  - **Machine learning-based malware detection**
  - **Malware family classification using machine learning**

Course Objectives

Upon completion of this course, you should be able to

1) Understand and be able to articulate the principles of computer security
2) Conduct research and utilize analytical skills for detecting malware or classifying malware families
3) Identify and describe best practices related to malware analysis
   - explaining the state-of-the-art methodologies in malware detection/analysis
   - modeling threats related to malware and their countermeasures
4) Discuss some case studies including the cutting-edge research on malware detections, preventions, and countermeasures.
5) Write a formal report detailing malware analysis

Requirements

- Course materials
  - Research papers
- Students must read 2 or more papers and present them.
  - Paper list will be given
  - You can select high quality papers
    - Journal papers, or Top-level conferences papers through Google Scholar
    - ☞ Top-level conferences: USENIX Security, ACM CCS, IEEE S&P, NDSS
- Read the followings
  - How to read a (research) paper (See the next slide)
    - https://web.stanford.edu/class/ee384m/Handouts/HowtoReadPaper.pdf (S. Keshav)
    - https://www.eecs.harvard.edu/~michaelm/postscripts/ReadPaper.pdf
    - https://www.elsevier.com/connect/infographic-how-to-read-a-scientific-paper
  - How to write a research paper

How to read a papers

- The three-pass approach
- **Some initial guidelines**
  - Read critically, Read creatively
  - Make notes as you read the paper
  - After the first read-through, try to summarize the paper in one or two sentences
  - If possible, compare the paper to other works
    - Doing a literature survey
  - Find out any limitations or extensions you see for the ideas in the paper
  - Suggest your opinion of the paper; primarily, the quality of the ideas and its potential impact

- YouTube
  - How to read a paper efficiently (By Prof. Pete Carr)
  - How to read a research paper (Siraj Raval)

Class rules

- Paper selection & Presentation
  - Read high quality papers related to malware analysis
  - 발표주제 선정, 발표 날짜 및 발표 시간 엄수
    - 발표 날짜 약속 불이행 시: 학점 상한제 도입
      - 2 weeks delay presentation: under B+,
      - 3 weeks delay presentation: under C+
    - 발표 시간: 1인 최소 30분 이상

- **Every student must to present the paper on a designated date.**

  If not, he fails

- 토론 및 질문 장려
  - 좋은 질문 및 수업태도에는 가산점
  - **Exceptional work will be awarded as appropriate**

Grade Breakdown

Tentative grading (subject to change)

- **Presentation/Discussion: 50%**
  - Paper read and presentation
  - Every student is recommended to ask question(s) to the presenter.
- **Assignment / Summary report: 15%**
  - Summary of the papers presented by others
  - Some quizzes
- **Final Exam: 25%**
- **Attendance: 10%**

Course Content

- Microsoft STRIDE model
- Security Properties
  - Confidentiality, Integrity, Availability, Authentication, Authorization, …
- The latest trends in cyber security
  - Emerging issues, trends, technologies and threats in cyber security.
  - Cybersecurity Trends in 2019/2020, or Top cybersecurity issues
- Reverse engineering
  - Static analysis vs. Dynamic analysis
- Android malware detection/analysis using machine learning
  - Feature extraction / Feature selection
  - Machine learning models: SVM, DT, RF, k-NN, DNN, CNN, …
  - Classifying Android malware families (Plankton, KMin, SMSsend, BaseBridge, DroidKungFu, …)
  - Other issues: Reliable ground truth dataset, N-fold cross validation, Grayware, False alarm reduction
- Malware analysis evasion techniques
  - code obfuscation, packing, file-less malware, anti-debugging, cross platform development
- Overview of adversarial example and adversarial attack

Recommended Papers

1. Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., Rieck, K., & Siemens, C. E. R. T. (2014, February). **Drebin: Effective and explainable detection of android malware in your pocket**. In *Ndss* (Vol. 14, pp. 23-36). (1196회)
2. Wei, F., Li, Y., Roy, S., Ou, X., & Zhou, W. (2017, July). **Deep ground truth analysis of current android malware**. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 252-276). Springer, Cham. (123회)
3. Allix, K., Bissyandé, T. F., Klein, J., & Le Traon, Y. (2016, May). **Androzoo: Collecting millions of android apps for the research community**. In *2016 IEEE/ACM 13th Working Conference on Mining Software Repositories (MSR)* (pp. 468-471). IEEE. (211회)
4. Dini, G., Martinelli, F., Saracino, A., & Sgandurra, D. (2012, October). **MADAM: a multi-level anomaly detector for android malware**. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security* (pp. 240-253). Springer, Berlin, Heidelberg. (423회)
5. Zhang, M., Duan, Y., Yin, H., & Zhao, Z. (2014, November). **Semantics-aware android malware classification using weighted contextual api dependency graphs**. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security* (pp. 1105-1116). (319회)
6. Sahs, J., & Khan, L. (2012, August). **A machine learning approach to android malware detection**. In *2012 European Intelligence and Security Informatics Conference* (pp. 141-147). IEEE. (287회)
7. Gascon, H., Yamaguchi, F., Arp, D., & Rieck, K. (2013, November). **Structural detection of android malware using embedded call graphs**. In *Proceedings of the 2013 ACM workshop on Artificial intelligence and security* (pp. 45-54). (252회)

Recommended Papers

8. Narudin, F. A., Feizollah, A., Anuar, N. B., & Gani, A. (2016). **Evaluation of machine learning classifiers for mobile malware detection**. *Soft Computing*, *20*(1), 343-357. (164회)
9. Yuan, Z., Lu, Y., & Xue, Y. (2016). **Droiddetector: android malware characterization and detection using deep learning**. *Tsinghua Science and Technology*, *21*(1), 114-123. (163회)
10. Li, J., Sun, L., Yan, Q., Li, Z., Srisa-an, W., & Ye, H. (2018). **Significant permission identification for machine-learning-based android malware detection**. *IEEE Transactions on Industrial Informatics*, *14*(7), 3216-3225. (146회)
11. Huang, C. Y., Tsai, Y. T., & Hsu, C. H. (2013). **Performance evaluation on permission-based detection for android malware**. In *Advances in Intelligent Systems and Applications-Volume 2* (pp. 111-120). Springer, Berlin, Heidelberg. (118회)
12. Yerima, S. Y., Sezer, S., & McWilliams, G. (2014). **Analysis of Bayesian classification-based approaches for Android malware detection**. *IET Information Security*, *8*(1), 25-36. (111회)
13. Milosevic, N., Dehghantanha, A., & Choo, K. K. R. (2017). Machine learning aided Android malware classification. *Computers &Electrical Engineering*, *61*, 266-274. (102회)
14. Dash, S. K., Suarez-Tangil, G., Khan, S., Tam, K., Ahmadi, M., Kinder, J., & Cavallaro, L. (2016, May). **Droidscribe: Classifying android malware based on runtime behavior**. In *2016 IEEE Security and Privacy Workshops (SPW)* (pp. 252-261). IEEE. (101회)
15. Suarez-Tangil, G., Dash, S. K., Ahmadi, M., Kinder, J., Giacinto, G., & Cavallaro, L. (2017, March). **Droidsieve: Fast and accurate classification of obfuscated android malware**. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy* (pp. 309-320). (92회)

Recommended Papers

16. Yerima, S. Y., Sezer, S., & Muttik, I. (2015). **High accuracy android malware detection using ensemble learning**. *IET Information Security*, *9*(6), 313-320. (91회)
17. Tahan, G., Rokach, L., & Shahar, Y. (2012). **Mal-id: Automatic malware detection using common segment analysis and meta-features**. *Journal of Machine Learning Research*, *13*(Apr), 949-979. (80회)
18. Spreitzenbarth, M., Schreck, T., Echtler, F., Arp, D., & Hoffmann, J. (2015). **Mobile-Sandbox: combining static and dynamic analysis with machine-learning techniques**. *International Journal of Information Security*, *14*(2), 141-153. (79회)
19. Demontis, A., Melis, M., Biggio, B., Maiorca, D., Arp, D., Rieck, K., ... & Roli, F. (2017). **Yes, machine learning can be more secure! a case study on android malware detection**. *IEEE Transactions on Dependable and Secure Computing*. (78회)
20. Chen, S., Xue, M., Tang, Z., Xu, L., &Zhu, H. (2016, May). **Stormdroid: A streaminglized machine learning-based system for detecting android malware**. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (pp. 377-388). (74회)
21. Roy, S., DeLoach, J., Li, Y., Herndon, N., Caragea, D., Ou, X., ... &Guevara, N. (2015, December). **Experimental study with real-world data for android app security analysis using machine learning**. In *Proceedings of the 31st Annual Computer Security Applications Conference* (pp. 81-90). (59회)
22. Karbab, E. B., Debbabi, M., Derhab, A., &Mouheb, D. (2018). **MalDozer: Automatic framework for android malware detection using deep learning**. *Digital Investigation*, *24*, S48-S59. (45회 인용)

Recommended Papers

23. Chen, X., Li, C., Wang, D., Wen, S., Zhang, J., Nepal, S., ... & Ren, K. (2019). **Android HIV: A study of repackaging malware for evading machine-learning detection**. *IEEE Transactions on Information Forensics and Security*, *15*, 987-1001.
24. Chen, L., Hou, S., Ye, Y., & Chen, L. (2017, July). **An adversarial machine learning model against android malware evasion attacks**. In *Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint Conference on Web and Big Data* (pp. 43-55). Springer, Cham.
25. Qiu, J., Nepal, S., Luo, W., Pan, L., Tai, Y., Zhang, J., & Xiang, Y. (2019, September). **Data-Driven Android Malware Intelligence: A Survey**. In *International Conference on Machine Learning for Cyber Security* (pp. 183-202). Springer, Cham.
26. Ma, Z., Ge, H., Liu, Y., Zhao, M., & Ma, J. (2019). **A combination method for android malware detection based on control flow graphs and machine learning algorithms**. *IEEE access*, *7*, 21235-21245.
27. Mahindru, A., & Singh, P. (2017, February). **Dynamic permissions based android malware detection using machine learning techniques**. In *Proceedings of the 10th innovations in Software Engineering Conference* (pp. 202-210).
28. Baskaran, B., & Ralescu, A. (2016). **A study of android malware detection techniques and machine learning**.
29. Abaid, Z., Kaafar, M. A., & Jha, S. (2017, October). **Quantifying the impact of adversarial evasion attacks on machine learning based android malware classifiers**. In *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)* (pp. 1-10). IEEE.
30. Yerima, S., Sezer, S., & Alzaylaee, M. K. (2017, March). **EMULATOR vs REAL PHONE: Android Malware Detection Using Machine Learning**. ACM.

Recommended Papers

31. Li, L., Gao, J., Hurier, M., Kong, P., Bissyandé, T. F., Bartel, A., ... &Traon, Y. L. (2017). **Androzoo++: Collecting millions of android apps and their metadata for the research community**. *arXiv preprint arXiv:1709.05281*. (28회)
32. Chen, L., Hou, S., &Ye, Y. (2017, December). **Securedroid: Enhancing security of machine learning-based detection against adversarial android malware attacks**. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (pp. 362-372). (27회)
33. Yerima, S. Y., &Sezer, S. (2018). **Droidfusion: A novel multilevel classifier fusion approach for android malware detection**. *IEEE transactions on cybernetics*, *49*(2), 453-466. (24회)
34. Wu, S., Wang, P., Li, X., &Zhang, Y. (2016). **Effective detection of android malware based on the usage of data flow APIs and machine learning**. *Information and software technology*, *75*, 17-25. (61회)
35. Chan, P. P., &Song, W. K. (2014, July). **Static detection of Android malware by using permissions and API calls**. In *2014 International Conference on Machine Learning and Cybernetics* (Vol. 1, pp. 82-87). IEEE. (56회)
36. Zarni Aung, W. Z. (2013). **Permission-based android malware detection**. *International Journal of Scientific &Technology Research*, *2*(3), 228-234. (224회)
37. Wu, W. C., &Hung, S. H. (2014, October). **DroidDolphin: a dynamic Android malware detection framework using big data and machine learning**. In *Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems* (pp. 247-252). (107회)
38. Peiravian, N., &Zhu, X. (2013, November). **Machine learning for android malware detection using permission and api calls**. In *2013 IEEE 25th international conference on tools with artificial intelligence* (pp. 300-305). IEEE. (226회)

Any questions?

- Hardships, The way of suffering
  - Passion, An unremitting effort, Sincerity, Diligence

- Expert, Specialist