Εργαστήριο Επιχειρηματικής Αναλυτικής
Οικονομικό Πανεπιστήμιο Αθηνών

Αλεξόπουλος Νικόλαος

alexopoulos@aueb.gr
https://www.balab.aueb.gr/nikolaos-alexopoulos.html

Ανοιχτά ερευνητικά θέματα στον τομέα της ασφάλειας λογισμικού:
Open reasearch topics in the area of SW security:

---

1. Realistic evaluation of ML-based static analysis tools

Background:
There are many bugs everywhere. Some of them are potentially security critical aka *vulnerabilities*. We need tools to help us find them. One of the approaches is using ML models to pinpoint “dangerous” parts of the code that are potentially vulnerable.

Problem:
Although there are many approaches proposed in literature (e.g. LineVul, SySeVR, FUNDED), their evaluation is lacking (biases like synthetic data, dataset balance, etc.). There are doubts about the actual effectiveness of proposed approaches in practice.

Goal:
Devise a realistic evaluation framework for testing the effectiveness of static analysis tools. Implement the framework incl. the required data collection and evaluate a selection of state-of-the-art ML-based approaches for vulnerability detection.

Prerequisites:
Basic knowledge of SW security and ML concepts, some programming experience, some data analysis knowledge.

Starting bibliography:
[1] Chen, Yizheng, et al. "Diversevul: A new vulnerable source code dataset for deep learning based vulnerability detection." Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. 2023. http://people.eecs.berkeley.edu/~daw/papers/diversevul-raid23.pdf.
[2] Michael Fu and Chakkrit Tantithamthavorn. “LineVul: A Transformer-based Line-Level Vulnerability Prediction”. In: 19th IEEE/ACM International Conference on Mining Software Repositories, MSR 2022. https://michaelfu1998-create.github.io/papers/linevul.pdf.

---

2. Privacy evaluation of Android system apps

Background:
Mobile devices comprise a large number of software from different vendors. Some of this (of course proprietary) software comes pre-installed and/or runs with elevated privileges, raising privacy and security concerns.

Problem:
Analysis of app permissions and network behavior has shown that system apps (even Google's default phone and messenger apps) transmit sensitive data to third-party servers.

Goal:
Leveraging advances in system tracing approaches (ftrace, ebpf) design a dynamic analysis system and deploy it to different devices in order to analyze runtime differences of respective system apps.

Prerequisites:
Basic knowledge of SW security, Linux kernel and Android concepts, some programming experience, some data analysis knowledge.

Starting bibliography:
[1] Leith, Douglas J. "What Data Do The Google Dialer and Messages Apps On Android Send to Google?." International Conference on Security and Privacy in Communication Systems, 2022. https://www.scss.tcd.ie/doug.leith/privacyofdialerandsmsapps.pdf.
[2] Gamba, Julien, et al. "An analysis of pre-installed android software." 2020 IEEE symposium on security and privacy (SP). IEEE, 2020. https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/684/An_Analysis_of_Pre-installed_Android_Software_2019_EN.pdf.