HW8: Paper from 2016

1. *Reference*:

Ulfar Erlingsson

Data-driven Software Security: Models and Methods

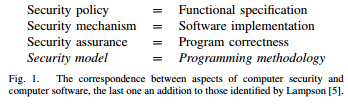
*Google, Inc., 2016*

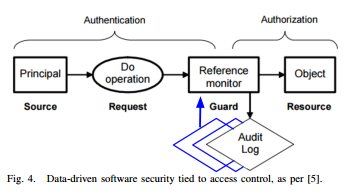
1. *Keywords*:
   1. **Software Security:**  The paper’s main focus is suggesting techniques of improving software security which have not ivolved as much as software engineering over the past five decades.
   2. **Security Models:** Security can never be ‘one size fits all’. Therefore the paper talks about providing a different security model for a different problem.
   3. **Data driven software security:** Since modern software have execution history attached to them, the paper sees it as an important piece of information and discuss how it can be used for better security.
   4. **RAPPOR:** An open source project used to collect execution trace data while preserving both anonymity and privacy of the user.
2. *Paper Contents:*
   1. **Motivational Statements**: (i) Permit only low-level executions that programmers intended to be possible, unless given explicit, special permission. (ii) Permit only executions that historical evidence shows to be common enough, unless given explicit, special permission.
   2. **Commentary**: Various existing open-source and popular scripts and libraries are used in this research:

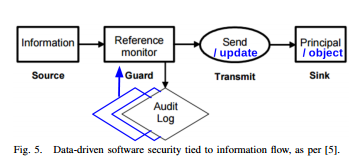
RAPPOR which is an open source Google project to a gather client side statistics but protecting user privacy and maintaining anonymity at the same time.

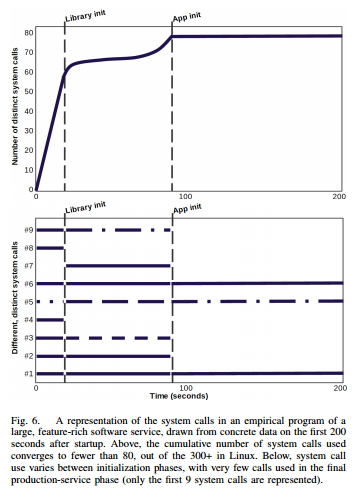
Standard technologies like ptrace and seccomp\_bpf can be used to effectively collect summarize and enforce system-call-trace-based security policies.

* 1. **Informative Visualizations**:









* 1. **Future work**: If issues like practical utility, efficiency and privacy can be fixed the model can serve as a breakthrough in software security. This has to be done using he current techniques such as reducing attack surface thus protecting the software in the same way as firewalls do.

1. *Needs Improvement:*
   1. The author, although emphasizes on an important point, misses out on any implementation details, applicability and deployment.
   2. The model raises concerns about the efficiency, practical utility and privacy.