CS 642: Midterm 2 Review Questions and General Study Pointers

April 2020

1 Anonymity

Review different notions of anonymity (e.g., dataset, communication, computation) and the techniques we use to achieve them. Also, review the Tor circuit setup protocol.

2 Software Security

- Review why code injection attacks can happen. E.g., unbounded buffer copy (strcpy), integer overflows (arithmetic in mixed-sign mode), format string vulnerabilities (sloppy use of printf).
- Go over your solutions to HW 4 to refresh your memory of the steps needed for the exploits.
- Review x86 instructions, including the RET and JMP instructions and their behavior/interaction with the stack.
- Review ASLR in detail. Spend some time reading the following paper: `https://hovav.net/ucsd/dist/asrandom.pdf`. Pay attention to how they calculate the probability of success of an attack on ASLR given various assumptions of randomization.
- Review program analysis methods to automate bug finding. E.g., static analysis tools like LINT, dynamic analysis techniques like fuzzing, symbolic execution, model checking.

3 Mobile Security

- What are Intents? Why are they crucial to how Android apps interact? What are the security issues if Intents are not used correctly?

- What is the Android app security model? Android apps run in their own execution context with their own UID. By default, this sandbox is locked down. If an app does not ask for any permissions, it will not be able access sensitive resources like GPS, microphone, etc.
- What is different about smartphone security vs. OS security (See slides, we went over this in a lot of detail)
- What kinds of permission models exist for smartphones? What are their advantages/disadvantages?

4 OS Security

- Review permission bits (rwxst) for owner, group, world. Also review setid bits and how to interpret. Work through the examples in slides. Test on your local linux machine to check understanding.
- What are the secure system design principles? E.g., least privilege, economy of mechanism, ...
- What is the difference between capabilities and access control list? (see slides)
- What are TOCTTOU, confused deputy attacks? (see slides)

5 Machine Learning

- What are the types of attacks on ML systems? Evasion (adversarial examples: change input image with small changes not noticeable to humans but make a large change in output). Poisoning (add poison instances to training data such that ML model learns some hidden functionality only known to attacker).
- What are privacy issues with ML? Membership inference, Model stealing.