Useful references for System Security Researchers

Below find links to expository papers, books, and useful tools that will help deepen your knowledge of the topics covered in class. Many of these references can also be very useful in regards to your project. While Wikipedia and Stack Overflow websites can act as brief starting points, you want to refer to the following papers/books to get a much deeper understanding of the topics discussed in class.

- **Papers on control-hijack and code-injection Attacks**
  - Art of Exploitation by Jon Erickson. One of the most comprehensive books on various kinds of attacks, although a bit outdated. Contains details about many different kinds of control hijack attacks and system security issues.
  - Return-2-libc attacks. A very good step-by-step guide to return-2-libc attacks.
  - Return-oriented programming (ROP) attacks. This is an excellent paper by Hovav Shacham and co-authors. Hovav invented ROP attacks.
  - Useful video on ROP attacks.

- **Papers on defense mechanisms**
  - Address Space Layout Randomization (ASLR). A detailed paper on analysis of an actual ASLR implementation.
  - Instruction Set Randomization (ISR) to protect against many forms of code-injection.
  - Control-flow Integrity (CFI) analysis.
  - Attack-resistant formal analysis of ASLR, ISR, and secure multi-execution. A high-level paper on attack-resistance.

- **Important disassembly/static/dynamic analysis, compiler infra tools**
  - IDA Pro: A powerful disassembly tool (commercial)
  - Coverity: Widely used static analysis tool (commercial)
  - PIN: x86 binary instrumentation tool useful in dynamic analysis
  - LLVM: Widely used compiler infra tool, dynamic/symbolic analysis

- **Widely used fuzzing and exploitation tools**
  - MetaSploit: a penetration testing, exploit construction tool
  - Fuzzing: An excellent resource on random, mutation, grammar fuzzing
- **Symbolic execution based analysis and testing**
  - KLEE: Most popular symbolic execution tool that uses STP
  - FuzzBall: Binary symbolic execution tool using STP
  - Companies developing their own symbolic execution tools: Google, Microsoft, IBM, HP Fortify, NVIDIA, Apple

- **SAT and SMT solvers used by security researchers**
  - Prominent SAT solvers: CryptoMiniSAT, Lingeling, Glucose, MapleSAT
  - Prominent SMT solvers: Z3, CVC4, Yices, STP, Z3str3