Instructors: Matt Fredrikson, Jean Yang TA: Samuel Yeom

Exam Date: March 9

Midterm Exam Topics

This is an outline of the topics that you should be familiar with for the 15-316 midterm exam. On March 7, we will go through selected topics during lecture, and answer any questions you have about these topics.

Note: You are allowed one cheat sheet (front and/or back) to bring in to the midterm!

The following topics are "fair game" for the exam.

- Basic security principles (complete mediation; least trust; minimal TCB)
- Safety
  - Formal definition of safety
  - Expressing safety properties using security automata
  - What are safety properties, and what are not
  - Inline reference monitors
    - Software fault isolation
    - Control flow integrity
  - What safety properties are used for in systems
  - Proof-carrying code
    - High-level motivation and mechanics of proof-carrying code
    - What the agent does, what the host does, what is trusted, etc.
    - What is the guarantee that proof-carrying code provides?
    - How would language extensions affect the proof rules and proofs?
    - What is trusted, what is not trusted
    - Understanding of the proof rules, and proof of soundness of the Safety Policy
- Authentication, authority, and trust
  - Formalism for proof-carrying authentication
  - Authentication logic, inference rules
  - Basic authentication proofs
  - The role of certificate authorities
  - Application of authorization logic to trusted software execution
- Information flow
  - Informal high-level definition of information flow
  - Process-level information flow with Flume
  - Conservative approximations of information flow with reference monitors

  - Basic information flow type system from class
  - Technique for proving soundness of the information flow type system
  - How would language extensions affect our information flow type system and proofs?

Techniques you should be familiar with include the following:

- Using automata to specify safety properties
- Proofs using our proof-carrying authentication logic
- Typing rules, derivations, and proof techniques for our information flow type system
- Proof rules and proof of soundness for the safety policy in PCC