Lecture 2 Outline

March 31, 2016

Reading: *text*, §2, 16.1–16.3 **Assignments due:** Homework 1, on Apr. 5

1. Greetings and felicitations!
2. Access Control Matrix
   a. Subjects, objects, and rights
   b. Primitive commands
   c. Commands and conditions: create-file, various flavors of grant-right to show conditions and nested commands
3. Decidability of security
   a. Notion of leakage in terms of ACM
   b. Determining security of a generic system with generic rights and mono-operational commands is decidable
   c. Determining security of a generic system with generic rights is undecidable (HRU result)
   d. Meaning: can't derive a generic algorithm; must look at (sets of) individual case
4. Access Control Lists
   a. UNIX method
   b. Full ACLs: describe, revocation issue
5. Capabilities
   a. Capability-based addressing
   b. Inheritance of C-Lists
6. Lock and Key
   a. Associate with each object a lock; associate with each process that has access to object a key (it's a cross between ACLs and C-Lists)
   b. Example: cryptographic (Gifford). X object enciphered with key K. Associate an opener R with X. Then:
      OR-Access: K can be recovered with any D_i in a list of n deciphering transformations, so
      $R = (E_1(K), E_2(K), \ldots, E_n(K))$ and any process with access to any of the D_i's can access the file
      AND-Access: need all n deciphering functions to get K: $R = E_1(E_2(\ldots En(K)\ldots))$
   c. Types and locks