“Security is economics.”
What does this program do?
What can this program do?

Can it delete all of your files? YES. Why?
“Least privilege.”
Touchstones for Least Privilege

• When assessing the security of a system’s design, identify the *Trusted Computing Base* (**TCB**).
  – What components does security rely upon?

• Security requires that the TCB:
  – Is *correct*
  – Is *complete* (can’t be bypassed)
  – Is itself *secure* (can’t be tampered with)

• Best way to be assured of correctness and its security?
  – **KISS** = *Keep It Simple, Stupid!*
  – Generally, *Simple* = **Small**

• One powerful design approach: *privilege separation*
  – Isolate privileged operations to as small a component as possible
  – (See lecture notes for more discussion)
Check for Understanding

• We’ve seen that PC platforms grant applications a lot of privileges
• Quiz: Name a platform that does a better job of least privilege
“Ensure complete mediation.”
Ensuring Complete Mediation

• To secure access to some capability/resource, construct a reference monitor
• Single point through which all access must occur
  – E.g.: a network firewall
• Desired properties:
  – Un-bypassable (“complete mediation”)
  – Tamper-proof (is itself secure)
  – Verifiable (correct)
  – (Note, just restatements of what we want for TCBs)
• One subtle form of reference monitor flaw concerns race conditions …
procedure withdrawal(w)
  // contact central server to get balance
  1. let b := balance

  2. if b < w, abort

  // contact server to set balance
  3. set balance := b - w

  4. dispense $w to user

TOCTTOU = Time of Check To Time of Use
public void buyItem(Account buyer, Item item) {
    if (item.cost > buyer.balance)
        return;
    buyer.possessions.put(item);
    buyer.possessionsUpdated();
    buyer.balance -= item.cost;
    buyer.balanceUpdated();
}