Why Compromises Matter - Access Control

User Access Control

What files can user read and/or write?
What programs can the user run?

Root or Administrator account
Can access everything
"superuser"

Normal users
Windows & Unix/Linux allow user groups to be
set up to say what "extra" access users in
that group have
Default is to just give access to user's own files/programs
& to "system-wide" programs
Risk - privilege escalations

Root kits
Any program that acts w/ superuser privileges
often hide their presence by changing system programs

Anomaly based intrusion detection
Detect "abnormal" behavior
Also called heuristic-based intrusion detection