Lecture 24: The Insider

Date: November 22, 2013 ***Homework Due***: Dec. 6 at 5:00pm

1. What is an “insider”?
   a. Masquerader
   b. Traitor
   c. Notion of “perimeter”
2. Types of insider attacks
   a. Misuse of access
   b. Bypassing defenses
   c. Access control failure
3. Technological solutions: detection
   a. Policy languages (especially formal ones)
   b. Misuse and anomaly techniques
   c. Decoys
   d. Markers
   e. Data exfiltration prevention
   f. Access controls (especially Role-Based Access Control, RBAC)
   g. Trusted systems
4. Human solutions: detection and prevention
   a. Policies: languages and hierarchies
   b. Monitoring
   c. Forensics
5. Human solutions: predictive
   a. Taxonomies and their uses
   b. Attack-related symptoms and behaviors
   c. Semantic analysis
   d. Motivational analysis
6. Legal considerations
7. Response