Outline: Lecture 9

Date: April 26, 2011
Topic: Detecting and Blocking Attacks

1. Access Control
   a. Basic Forms
      i. Mandatory
      ii. Discretionary
      iii. Originator-Controlled
   b. Conditional
   c. Dynamic
      i. Based on History
      ii. Optimistic
2. Intrusion Detection
   a. Anomaly Detection
   b. Misuse Detection
   c. Signature Detection
   d. Host-Based
   e. Network-Based
   f. Distributed
3. Buzzword "Compliance"
   a. Intrusion Prevention
   b. Unified Threat Model (UTM)
   c. Advanced Persistent Threat (APT) Detection