Review of DBMS Security

Match security mechanism (1) through (7) with security threats (a) through (h):

• Security Mechanisms
  – (1) discretionary access control (e.g. GRANT/REVOKE),
  – (2) mandatory access control (e.g. Bell LaPadula model, multi-level relations)
  – (3) statistical inference control (e.g. add i.i.d noise to sensitive fields),
  – (4) Encryption,
  – (5) External security software, e.g. Oracle VPN-based labels,
  – (6) Use prepared (pre-compiled) parametric SQL statements in applications,
  – (7) Analyze DBMS-logs for anomalous patterns.

• Security Threats:
  – (a) Unauthorized user queries a sensitive field (e.g. grades).
  – (b) Unauthorized program (e.g. trojan horse, virus) queries a sensitive field.
  – (c) Data miner infers confidential individual data from public aggregates.
  – (d) Insider Attack, DBA reads salaries of all executives.
  – (e) Data-flow: Authorized user emails data to unauthorized user (wiki-leaks).
  – (f) SQL Injection attack.
  – (g) Information-flow: Authorized users send bits of information
to unauthorized users using signals (e.g. overload DBMS server).
  – (h) Dumpster diving: Unauthorized person finds a worn-out backup tape in garbage.
  – He recovers credit-card numbers from readable portions of tape.