Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
        B set of current accesses (*i.e.*, access modes each subject has currently to each object);
        M access permission matrix;
        F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
        H hierarchy of system objects, functions h: O->$P(O)$ with two properties:
        If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
        There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
        B set of current accesses (*i.e.*, access modes each subject has currently to each object);
        M access permission matrix;
        F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
        H hierarchy of system objects, functions h: O->$P(O)$ with two properties:
        If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
        There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \varnothing$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
       B set of current accesses (*i.e.*, access modes each subject has currently to each object);
       M access permission matrix;
       F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
       H hierarchy of system objects, functions $h: O \rightarrow P(O)$ with two properties:
       If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
       There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
       B set of current accesses (*i.e.*, access modes each subject has currently to each object);
       M access permission matrix;
       F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
       H hierarchy of system objects, functions $h: O \rightarrow P(O)$ with two properties:
       If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
       There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples

2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B{\times}M{\times}F{\times}H$ where:
       B set of current accesses (*i.e.*, access modes each subject has currently to each object);
       M access permission matrix;
       F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
       H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
       If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
       There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{\, o_1, \ldots, o_k \,\} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{\, o_1, \ldots, o_k \,\} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples

2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O \text{->} P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \varnothing$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: O->$P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
        B set of current accesses (*i.e.*, access modes each subject has currently to each object);
        M access permission matrix;
        F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
        H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
        If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
        There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\rightarrow}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{\, o_1, \ldots, o_k \,\} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: O->$P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \varnothing$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O\text{->}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
   B set of current accesses (*i.e.*, access modes each subject has currently to each object);
   M access permission matrix;
   F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
   H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
   If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
   There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples

2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
        B set of current accesses (*i.e.*, access modes each subject has currently to each object);
        M access permission matrix;
        F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
        H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
        If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
        There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
        B set of current accesses (*i.e.*, access modes each subject has currently to each object);
        M access permission matrix;
        F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
        H hierarchy of system objects, functions h: O->$P(O)$ with two properties:
        If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
        There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
        B set of current accesses (*i.e.*, access modes each subject has currently to each object);
        M access permission matrix;
        F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
        H hierarchy of system objects, functions h: O->$P(O)$ with two properties:
        If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
        There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\to}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B \times M \times F \times H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O \rightarrow P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B{\times}M{\times}F{\times}H$ where:
       B set of current accesses (*i.e.*, access modes each subject has currently to each object);
       M access permission matrix;
       F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
       H hierarchy of system objects, functions h: $O{-}{>}P(O)$ with two properties:
       If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
       There is no set $\{\, o_1, \ldots, o_k \,\} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
   a. Labels and regions
   b. Multilevel directories
   c. File object labels
   d. MAC tuples
2. BLP: formally
   a. Elements of system: s_i subjects, o_i objects
   b. State space $V = B{\times}M{\times}F{\times}H$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
      H hierarchy of system objects, functions h: $O{\rightarrow}P(O)$ with two properties:
      If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
      There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R{\times}D{\times}V{\times}V$ is motion from one state to another.

Outline for April 20, 2004

1. Example: DG/UX UNIX
    a. Labels and regions
    b. Multilevel directories
    c. File object labels
    d. MAC tuples
2. BLP: formally
    a. Elements of system: s_i subjects, o_i objects
    b. State space $V = B \times M \times F \times H$ where:
        B set of current accesses (*i.e.*, access modes each subject has currently to each object);
        M access permission matrix;
        F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
        H hierarchy of system objects, functions h: $O \to P(O)$ with two properties:
        If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
        There is no set $\{ o_1, \ldots, o_k \} \subseteq O$ such that for each i, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$.
    c. Set of requests is R
    d. Set of decisions is D
    e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.