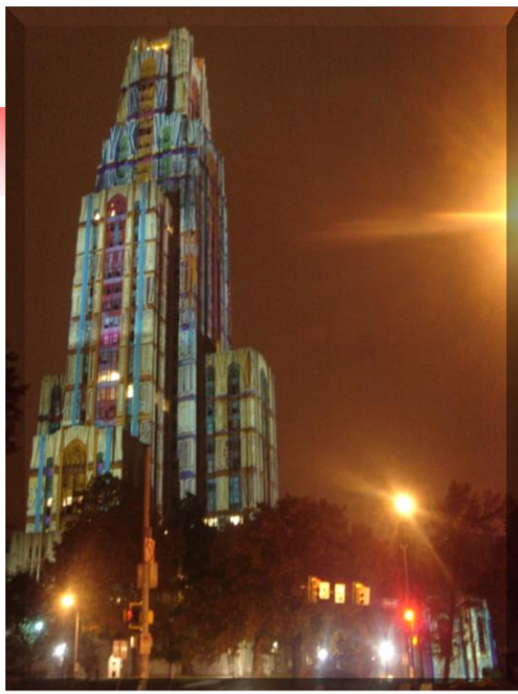
IS 2150 / TEL 2810
Information Security & Privacy



James Joshi

Associate Professor, SIS

Lecture 3.1

Jan 23, 2013

Mathematical Review

Security Policies

Objective

- Review some mathematical concepts
  - Propositional logic
  - Predicate logic
  - Mathematical induction
  - Lattice

Propositional logic/calculus

- Atomic, declarative statements (propositions)
  - that can be shown to be either TRUE or FALSE but not both; E.g., "Sky is blue"; "3 is less than 4"
- Propositions can be composed into compound sentences using connectives
  - Negation $\neg p$ (NOT) highest precedence
  - Disjunction $p \vee q$ (OR) second precedence
  - Conjunction $p \wedge q$ (AND) second precedence
  - Implication $p \rightarrow q$ q logical consequence of p
- Exercise: Truth tables?

Propositional logic/calculus

- Contradiction:
  - Formula that is always false : $p \wedge \neg p$
  - What about: $\neg(p \wedge \neg p)$?
- Tautology:
  - Formula that is always True : $p \vee \neg p$
    - What about: $\neg(p \vee \neg p)$?
- Others
  - Exclusive OR: $p \oplus q$; p or q but not both
  - Bi-condition: $p \leftrightarrow q$ [p *if and only if* q (p iff q)]
  - Logical equivalence: $p \Leftrightarrow q$ [p is logically equivalent to q]
- Some exercises…

Some Laws of Logic

- Double negation
- DeMorgan's law
  - $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$
  - $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
- Commutative
  - $(p \vee q) \Leftrightarrow (q \vee p)$
- Associative law
  - $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$
- Distributive law
  - $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
  - $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

Predicate/first order logic

- Propositional logic
- Variable, quantifiers, constants and functions
- Consider sentence: *Every directory contains some files*
- Need to capture “every” “some”
  - F(x): x is a file
  - D(y): y is a directory
  - C(x, y): x is a file in directory y

Predicate/first order logic

- Existential quantifiers $\exists$ (There exists)
  - E.g., $\exists x$ is read as There exists x
- Universal quantifiers $\forall$ (For all)
- $\forall y \; D(y) \rightarrow (\exists x \, (F(x) \wedge C(x, y)))$
- read as
  - for every y, *if* y is a directory, then there exists a x such that x *is a file* and *x is in directory y*
- What about $\forall x \; F(x) \rightarrow (\exists y \, (D(y) \wedge C(x, y)))$?

Mathematical Induction

- Proof technique - to prove some mathematical property
    - E.g. want to prove that M(n) holds for all natural numbers
  - Base case OR Basis:
    - Prove that M(1) holds
  - Induction Hypothesis:
    - Assert that M(n) holds for $n = 1, \ldots, k$
  - Induction Step:
    - Prove that if M(k) holds then M(k+1) holds

Mathematical Induction

- Exercise: prove that sum of first n natural numbers is
  - S(n): $1 + \ldots + n = n(n + 1)/2$
- Prove
  - S(n): $1^2 + \ldots + n^2 = n(n+1)(2n + 1)/6$

Lattice

- Sets
  - Collection of unique elements
  - Let S, T be sets
    - Cartesian product: S x T = {(a, b) | a ∈ A, b ∈ B}
    - A set of order pairs
- Binary relation R from S to T is a subset of S x T
- Binary relation R on S is a subset of S x S
- If (a, b) ∈ R we write aRb
  - Example:
    - R is "less than equal to" (≤)
    - For S = {1, 2, 3}
      - Example of R on S is {(1, 1), (1, 2), (1, 3), ????)
  - (1, 2) ∈ R is another way of writing 1 ≤ 2

Lattice

- Properties of relations
  - Reflexive:
    - if a*R*a for all $a \in S$
  - Anti-symmetric:
    - if a*R*b and b*R*a implies a = b for all $a, b \in S$
  - Transitive:
    - if a*R*b and b*R*c imply that a*R*c for all $a, b, c \in S$
  - Which properties hold for "less than equal to" ($\leq$)?
  - Draw the Hasse diagram
    - Captures all the relations

Lattice

- Total ordering:
  - when the relation orders all elements
  - E.g., “less than equal to” (≤) on natural numbers
- Partial ordering (poset):
  - the relation orders only some elements not all
  - E.g. “less than equal to” (≤) on complex numbers; Consider (2 + 4i) and (3 + 2i)

Lattice

- Upper bound $(u, a, b \in S)$
  - u is an upper bound of a and b means aRu and bRu
  - Least upper bound : $lub(a, b)$ *closest upper bound*
- Lower bound $(l, a, b \in S)$
  - l is a lower bound of a and b means lRa and lRb
  - Greatest lower bound : $glb(a, b)$ *closest lower bound*

Lattice

- A lattice is the combination of a set of elements *S* and a relation *R* meeting the following criteria
  - R is reflexive, antisymmetric, and transitive on the elements of S
  - For every $s, t \in$ S, there exists a greatest lower bound
  - For every $s, t \in$ S, there exists a lowest upper bound
- Some examples
  - S = {1, 2, 3} and R = $\leq$?
  - S = {2+4i; 1+2i; 3+2i, 3+4i} and R = $\leq$?

Overview of Lattice Based Models

- Confidentiality
  - Bell LaPadula Model
    - First rigorously developed model for high assurance - for military
    - Objects are classified
    - Objects may belong to Compartments
    - Subjects are given clearance
    - Classification/clearance levels form a lattice
    - Two rules
      - No read-up
      - No write-down