CS590N
Logical Methods in Information Security

Lecture 1 (Jan 07)
Introduction to the Course
Instructor Info

- Ninghui Li
  - Email: ninghui@cs.purdue.edu
  - Office phone: 765-496-6756
  - Office: LWSN 2142K

- Office hour
  - After lectures on Mondays, Wednesdays
  - And by appointment
Coursework

- Regular attendance
  - including an extra lecture slot
- Readings before some lectures
- A few homework assignments (30%)
- Mid-term exam (30%)
- Presentations (10%)
- A project (30%)
Textbook and Resources

- Logic in Computer Science, 2\textsuperscript{nd} Edition
  - Michael Huth and Mark Ryan
  - homework may be in the book

- Learning Prolog Now
  - [http://www.coli.uni-saarland.de/~kris/learn-prolog-now/](http://www.coli.uni-saarland.de/~kris/learn-prolog-now/)

- Papers
Factoring Computer Security

- Cryptography
  - Encryption, signatures, cryptographic hash, ...
- Security mechanisms
  - Access control policy
  - Network protocols
  - Defenses against software vulnerability attacks
- Implementation
  - Cryptographic library
  - Code implementing mechanisms
Where Logical Methods Are Used?

- Access control
  - policy specification and implementation
  - policy refinement, analysis, transformation
- Protocol analysis
- System vulnerability analysis
- Software vulnerability analysis
- Privacy
Most logics used in the design, specification, and verification of computer systems deal with a satisfaction relation

\[ M^2 \phi \]

- \( M \) describes the situation or model of a system
- \( \phi \) specifies what should be true
- \( ^2 \) can be implemented
Logical Methods

- Propositional logic SAT
- Logic programming
- Temporal logic and model checking
- Theorem proving
- Modal logic
- Description logic
- Fuzzy logic
- Multi-valued logic
- String rewriting
- ...
Goals of this course

- Learns the basics of the most widely used logic and logical methods

- Have a general idea about what kinds of security problems can be effectively solved using logical methods
Plan for the first several weeks

- Brief review of protocol analysis
- Prolog
  - Use Learning Prolog Now
- Using logic programming for protocol analysis
- Propositional logic
  - Use Logic in Computer Science
Future Plans

- First-order Logic
  - Use Logic in Computer Science
- More applications of logical methods to security
- Model checking
- Possibly description logic, fuzzy logic, multi-valued logic
- ...


Rest of this lecture

- Overview of Protocol Analysis
Coming Attractions

- Next 3 to 4 lectures will be on Prolog