

SYRACUSE UNIVERSITY
L.C. SMITH COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

CIS/CSE 774 – Principles of Distributed Access Control
Fall 2009

Catalog Description

Specification, verification, and design of secure networks using formal logic. Includes cryptographic algorithms and reasoning about key distribution protocols, delegation, access control, electronic mail, and certification authorities.

Instructor Information

Prof. Susan Older (sueo@ecs.syr.edu)

Office: CST 4-181, x4679

Office hours: Wednesdays (9:30-11:30am) or by appointment

Course Web Address

<http://www.cis.syr.edu/~sueo/774>

Textbook

For most of the semester, we will be using draft chapters of the following textbook:

Shiu-Kai Chin and Susan Older. *Access Control, Security, and Trust: A Logical Approach*. To be published by CRC Press in 2010.

I will provide hard copies of these chapters in class: please do not distribute them beyond the classroom. Additional relevant papers may be made available via the course web page.

Course Objectives

The primary goal of this course is to equip you to think rigorously about access control in distributed systems and to be able to rigorously assess the correctness of access-control policies, mechanisms, and trust topologies. In support of this goal, the educational objective is for you to acquire the ability to do formal analysis with an access-control calculus grounded in modal logic.

Prerequisites

To do well in this course, you must be familiar and comfortable with predicate logic, as well as sets and relations (à la CIS 275 or CSE 607). You must also be able to construct rigorous arguments/proofs about these topics and use induction where warranted.

More specifically, the knowledge required of predicate calculus at various levels are:

Comprehension

- When given a formula in predicate calculus and its interpretation, you should be able to explain its meaning in English.
- When given a precise but informal description, you should be able to represent the description symbolically and give its interpretation.

Analysis

- When given a set of assumptions and a goal to prove, you should be able to prove or disprove the goal, using the rules of inference to calculate whether the goal is true or not.
- When given a formula in predicate logic and a specific universe of discourse, determine the truth or falsity of the formula.
- When given definitions of operations on sets or relations, you should be able to calculate the result of applying those operations to specific sets.

Synthesis

- When given a set of assumptions and a (true) goal to prove within an underlying theory, you should be able to devise a proof strategy to prove the goal based on the form of the goal, the sorts, definitions, and theorems of the underlying theory.

Evaluation

- When given a theory, inference rules, and a proof, you should be able to judge if the proof is correct.

Course Outcomes

This course is an analytical course that uses predicate calculus and specialized logical systems to reason about distributed access control in a rigorous way. The specific educational outcomes at several levels of knowledge are:

Comprehension

- Define the meaning of security services such as confidentiality, integrity, non-repudiation, and authentication.
- Describe the characteristics of private-key and secret-key cryptographic systems.
- Describe basic principles of trust topologies and networks of certification authorities.
- Describe basic principles of security policies, both military (confidentiality) and commercial (integrity).
- Describe how address descriptors and protection descriptors are used for process isolation and memory segmentation.

Application

- When given protocol descriptions and trust hierarchies, you should be able to use the access-control logic to describe the protocol and trust relationships.
- When given a trust topology, you should be able to determine the necessary certificates for establishing trust in a key.
- When given a protocol description or a concept of operations for a distributed system relying on delegation, you should be able to identify the delegates and the statements on which they are trusted.
- When given a description of a memory-protection scheme using address and protection descriptors, you should be able to write down formulas in the access-control logic describing the interpretation of requests, tickets, descriptors, and protection policies enforced by the reference monitor.

Analysis

- When given a set of assumptions and a security goal to prove, you should be able to prove, using formal inference rules, whether the security goal is true or not.
- When given a Kripke structure, you should be able to determine the beliefs of principals (simple and compound) and whether or not one principal speaks for another.
- When given an axiom or theorem in the access-control logic, you should be able to prove its soundness in the underlying Kripke model.
- When given a set of certificates, you should be able to formally derive whether a key is associated with a particular principal.

Synthesis

- When given a “real life” scenario that incorporates delegation, certificates, and access control, you should be able to formally describe the scenario in the access-control logic and show how access-control decisions are made using the inference rules of the access-control logic.
- When given a description of a trust topology, you should be able to create a formal description of the certificates and trust relationships for the certification authorities.

Evaluation

- When given a theory, inference rules, and a proof, you should be able to judge if the proof is correct.
- When given a proposed inference rule, you should be able to judge whether or not it is sound.
- When given a specification and implementation, you should be able to judge whether the implementation satisfies its specification.

Outcome Measurement

Grades will be based on a combination of homework assignments and exams. I also expect students to attend class and will take participation into account when assigning final grades.

Homeworks (30% of final grade) are intended to keep you up-to-date with the material and to give you practice with the conceptual tools. There will be a homework assignment approximately every week. Unless otherwise noted, you are free to discuss the homeworks with others, *in accordance with the class honor policy*. Assignments are due by the date and time stated on them: **No late assignments will be accepted.**

The exams (70% of final grade) will allow you to demonstrate your understanding of the fundamental concepts. There will be three in-class exams during the semester. There will also be a two-hour *optional* final exam: the exam portion of your final grade will be the greater of (1) your cumulative average of the in-class exams, and (2) your score on the final exam.

Course Topics

Modal access-control logic, including Kripke structures, inference rules, and soundness. Access-control concepts, including reference monitors, access-control matrices, access lists, and tickets/capabilities. Delegation, authorization, PKI and certificate authorities, chains of trust. Process isolation and sharing. Virtual machines.

Other Information

Academic Integrity

I expect all students to behave with academic integrity: **do not cheat, plagiarize, or commit fraud**. Fraud includes faking program transcripts to make it appear that code works correctly when it does not; plagiarism includes using someone else's work without proper credit. If I discover any instances of cheating, fraud, or plagiarism, I will give the guilty parties **failing grades for the course** and report the culprits to the department chair and the Office of Academic Integrity. If you are unsure whether a certain action constitutes cheating, fraud, or plagiarism, assume that it does: you may ask us for clarification at any time.

Every student must read and sign a copy of the course **Honor Policy**, which details your obligations to behave ethically. Students will receive zeroes on all assignments/exams until this sheet is turned in to me.

Accommodations

Students who are in need of disability-related academic accommodations must register with the Office of Disability Services (ODS), 804 University Avenue, Room 309, 315-443-4498. Students with authorized disability-related accommodations should provide a current *Accommodation Authorization Letter* from ODS to the instructor and review those accommodations with the instructor. Accommodations, such as exam administration, are not provided retroactively; therefore, planning for accommodations as early as possible is necessary.

For further information, see the ODS website <http://disabilityservices.syr.edu>.