Course Web Page and Contact

- Course URL:
  - Google “Lingyu Wang” → Teaching
  - Important to visit this page regularly
  - Don’t depend on email notification

- Contact: wang@ciise.concordia.ca
  - The best way to reach me
  - Please include “INSE 6130” in your subject line
More Contact and Prerequisites

- More contact
  - Office: EV009.183
  - Office hours: See class webpage

- Prerequisites
  - INSE 6110
  - Basic knowledge of operating system
  - Discrete mathematics and formal notations
  - Web and PDF capable

Submission of Proposal and Report

- You must submit reports using the EAS:
  - No hard copy or email submission will be accepted
  - [https://fis.encs.concordia.ca/eas/](https://fis.encs.concordia.ca/eas/)
Textbook and References

  - Reading corresponding chapters (see class webpage) of the textbook is mandatory
- Other optional readings
  - Papers, e-book, web links on the class webpage
- Only the textbook is mandatory
  - But naturally, the more you read, the more you learn and the better grade you may get

Grading

- Academic Integrity
  - All students must follow the university's policies regarding academic integrity
  - I take the Code of Conduct very seriously!
  - I will do my best to identify any plagiarism in your report, and will have zero tolerance regarding this
    - I have proved this point in previous terms – so yes, it’s for real!
  - Take pride in your work (and self)
Grading

- Grading
  - Two exams (closed-book, 35% x 2)
  - A project (a proposal, a progress report, a final report, a presentation, 30%)
  - The final grade is based on curving the overall performance, but there is no direct mapping between numerical percentage grades and final letter grades for the course.

Project

- Group project
  - No smaller group size is allowed than what is specified in the project description! No exception
  - Your responsibility to organize, and work as, a team
    - A conflict will affect your mark, if I become aware of it
  - Anticipate and learn to deal with potential conflicts
    - Clearly divide and state each member’s responsibility as early as possible, and then stick to it
    - Make each member’s job less dependent on others’ outcome
  - In most cases, grade is given to a group, not individual
    - If there’s plagiarism in your report, then everyone will be responsible!
Project (Cont’d)

- Project Topic
  - See project description.
- Project proposal
  - To proceed, a 1-2 page proposal must be approved (see class webpage for deadline)
  - A clear description of the objective, the environment, the methodology, and the plan
  - One proposal per group, but it must clearly state each member’s responsibility
    - Be as specific as possible to avoid future conflicts

Project (Cont’d)

- A 6-7 page progress report (see class webpage for deadline)
  - Font size 11, single space, reasonable margins
  - One report per group, but it must list each member’s progress
- A 15-20 page final report (see class webpage for deadline)
  - Same format/requirement as the progress report
- A short presentation (see class webpage for the date)
  - One presentation per group
  - Detailed schedule will be given on the class webpage later
- Grading is based on the originality, clarity, and comprehensiveness of the presentation and final report, as well as on the timeliness of progress
Policies

- Again, be very serious about the code of conduct
  - Any kind of cheating/plagiarism will guarantee your group a grade of F
  - Everyone should check the report throughout before its submission
- Late submission policy
  - Late project reports will be accepted with 20% Penalty for each day past due up to five days
  - Late submission of proposal or progress report, or failure to present the project will also result in penalty on the group

Policies (Cont’d)

- Make-up exam possible ONLY:
  - Under a university-approved condition, such as sickness with the university doctor’s note. Other events such as, a business travel, family reunion, or wedding, are not excused. No exception.
  - You must write me before the normal exam date to arrange a make up exam.
  - What I can guarantee is
    - The make up exam will be completely different from the normal exam
  - What I can’t guarantee is
    - They will be of exactly the same difficulty
Course Description

- From the catalog
  - System security, MS Windows security, linux security, unix security, embedded and real-time OS, system reliability, OS security mechanisms, security administration, delegation of authority, group policy design, security configuration, password requirements, security services, protection models, protection levels, protection domains, capabilities, sharing, system kernel security, resource control, secure booting, firewalls and border security, security models and policies, security levels, authentication, confidentiality, integrity, access control strategies access matrix, access control list, mandatory, discretionary, monitoring, auditing, accountability, privilege, account security, file system protection, registry security, threat analysis, security attacks, security-hardened operating

- What to expect from this course
  - Foundational knowledge about system security
  - State of the art
  - State of the practice

- What not to expect
  - MCSE+Security, RHCSA/Security, COMP346, Hacker 101

Course Schedule

(Subject to change. Check class page for updates.)
Course Outline

- Introduction
  - Overview of all perspectives of system security: Objectives, threats, policies and mechanisms, the role of trust, assurance, operational issues, human issues
- Access Control Matrix and Foundational Results
  - ACM: simple yet (most) powerful security model
  - Transition in ACM
  - Safety question
  - HRU result
- Access Control Mechanism in UNIX
  - ACL, Capabilities, RBAC
  - ACL and Capabilities in UNIX and Windows
  - RBAC in Solaris

Course Outline (Cont’d)

- Security Policies and Confidentiality Policies
  - Overview of security policy
  - Bell-LaPadula (BLP) model
- Integrity Policies and Hybrid Policies
  - Biba model
  - Lipner’s model
  - Clark-Wilson model
  - Chinese Wall model
- Design principles and Unix Security
  - Principles of security design
  - User security in UNIX
  - File system security in UNIX
Course Outline (Cont’d)

- Secure Booting
  - Secure bootstrap architectures and TPM
- Authentication and Identity
  - Password security
  - Challenge response
  - Biometrics
- Auditing and Logging
  - Auditing systems
  - Auditing in UNIX
  - Audit log analysis
- Vulnerability and Defense
  - Common vulnerabilities
  - Intrusion detection

Course Outline (Cont’d)

- Securing Network Services
  - Security in UNIX internet server
  - Network Security tools in UNIX and Windows
  - Security protocols
- Various Topics
  - Registry security
  - Embedded and real-time OS security
  - Cloud computing security
  - Mobile OS security
INSE 6130 Operating System Security

Introduction

Prof. Lingyu Wang

What is computer security?

- Physical security vs. information security
  - Different, but share similar principles
- Is security
  - Password?
  - Encryption?
  - Virus/worm/botnet?
  - Firewall?
  - Hack(er)?
- The main objective of this course is to answer this question in a systematic way
Outline
- Objectives
- Threats
- Policies and mechanisms
- The role of trust
- Assurance
- Operational Issues
- Human Issues

Objectives
- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access
  - Data and resources
Examples

- **Commercial**
  - Confidentiality: An employee should not know others’ salary (maybe)
  - Integrity: An employee should not be able to modify his/her own salary
  - Availability: Paychecks should be printed on time as stipulated by law

- **Military**
  - Confidentiality: The target coordinates of a missile should not be improperly disclosed
  - Integrity: The target coordinates of a missile should not be improperly modified
  - Availability: When the proper command is issued the missile should fire

Classes of Threats

- **Disclosure**
  - Snooping (sniffing)

- **Deception**
  - Modification, spoofing (masquerading), repudiation of origin, denial of receipt

- **Disruption**
  - Modification

- **Usurpation**
  - Modification, spoofing, delay, denial of service (different from unavailability)

- What objectives are involved?
Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines “security” for the system
  - Natural language, math, special languages
- Mechanisms enforce policies
  - Technical or procedural
- OM-AM (by Ravi Sandhu)

<table>
<thead>
<tr>
<th>Objective (policy)</th>
<th>Confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>ACM</td>
</tr>
<tr>
<td>Architecture</td>
<td>Client-Server</td>
</tr>
<tr>
<td>Mechanism</td>
<td>Encryption</td>
</tr>
</tbody>
</table>

Ways for Achieving Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers’ violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds
Trust and Assumptions

- Underlie all aspects of security
- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy
  - Work correctly

Types of Mechanisms

- Secure
- Precise
- Broad

- set of reachable states
- set of secure states
Assurance
- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

Operational Issues
- Cost-Benefit Analysis
  - Is it cheaper to prevent or to recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect it?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people use them?
Human Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering

Tying Together

- Threats
  - Policy
    - Specification
      - Design
        - Implementation
          - Operation