CS 356 Systems Security  
Fall 2017  
http://www.cs.colostate.edu/~cs356

Dr. Indrajit Ray  
http://www.cs.colostate.edu/~indrajit

Administrivia

• Website: http://www.cs.colostate.edu/~cs356  
  – Syllabus outline  
  – Grading policy  
  – Homeworks  
  – Projects  
• CANVAS: mostly for quizzes, assignment and poster submissions and for keeping track of grades

Administrivia

• Instructor: Indrajit Ray  
  – Office: RM 344 COMSC  
  – Phone: (970) 491-7097  
  – Email: indrajit.ray@colostate.edu (best way to contact)  
  – Office hours:  
    • Tuesdays 11:00 am – 1:00 pm  
    • Or by appointment
Administrivia

- TA: Pratik Warade (main contact)
  - Email: pswarade@colostate.edu
- TA: Subhojeet Mukherjee (secondary)
  - Email: subhojeet.mukherjee@colostate.edu
- Office: Rm 120 CSB
  - Phone: (970) 491-7773
  - Office hours: TBD
- UTA: Noah Cain (for DETER Lab related)
  - Email: noah.mason.cain@gmail.com

Grading and Policies

- Grading
  - Class Participation 10%
  - Quizzes 25%
  - Poster 10%
  - Projects 15%
  - Midterm 20%
  - Final Exam 20%
- Grading policies
  - No credit for late projects. No exceptions
  - No makeup exams or quizzes. No exceptions
    - It is the student’s responsibility to check for conflicts for Midterm and Final exam and make necessary arrangements

Class Participation

- Regular attendance is required
  - Instructor and TA will keep track
  - Graded homework / project / exam not picked up by student in class on the day of return is a sign of non-attendance
- Students are expected to answer questions as well as ask
- Class scribes
  - Selected at the beginning of class. Be prepared to be a scribe.
Class Scribe

- Class scribes are responsible for taking notes, collectively editing the same and compiling into 1 PDF file for posting on CS 356 web site
  - Scribe notes should include (besides record of salient points mentioned on a topic) record of specific questions asked and answered during a lecture (TA will send list of questions asked during a lecture).
  - Scribe notes to be submitted to instructor and TA within 48 hours of end of class

Class Scribe (continued)

- Quality and completeness of note will contribute significantly towards score in class participation
- The entire class depends on you!!

Workload

- Weekly reading assignments
- Course Projects
  - Series of hands-on and programming exercises
- Weekly quizzes
  - Opened on Thursdays after class on CANVAS. Need to finished by beginning on class on next Tuesday.
- Exams
  - Midterm #1 20% of grade, Final Exam 20% of grade
  - Closed book, closed notes, in class exams
### Policies

<table>
<thead>
<tr>
<th>• Simple cheating policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Anyone caught cheating will <strong>FAIL the CLASS</strong></td>
</tr>
<tr>
<td>- Regardless of what you cheated in, so think carefully before you cheat.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• CS Academic Integrity Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <a href="http://www.cs.colostate.edu/advising/student-info.html">http://www.cs.colostate.edu/advising/student-info.html</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• Plagiarism – see definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <a href="http://writing.colostate.edu/guides/teaching/plagiarism/">http://writing.colostate.edu/guides/teaching/plagiarism/</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• Conflict Resolution web site</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <a href="http://www.conflictresolution.colostate.edu/">http://www.conflictresolution.colostate.edu/</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• ACNS acceptable use policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <a href="http://www.acns.colostate.edu/?page=aup">http://www.acns.colostate.edu/?page=aup</a></td>
</tr>
</tbody>
</table>

### Policies

<table>
<thead>
<tr>
<th>• No bad or disruptive behavior accepted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please familiarize yourself with the code of professional conduct for the CS department</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• Specially for male students</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Don’t bully or harass your female colleagues</td>
</tr>
<tr>
<td>- Read this blog from Professor Eugene Spafford: <a href="https://www.cerias.purdue.edu/site/blog/post/where_out_of_balance/">https://www.cerias.purdue.edu/site/blog/post/where_out_of_balance/</a></td>
</tr>
</tbody>
</table>

### Policies

<table>
<thead>
<tr>
<th>• No cell phone / smart phone use is acceptable in class. No exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>- The instructor will confiscate these devices and use them to support his research on mobile device security.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• Tablets and laptops can be used only for following the class lectures</th>
</tr>
</thead>
<tbody>
<tr>
<td>- The instructor reserves the right to use available technology to monitor potential violations of this code</td>
</tr>
</tbody>
</table>
Text, Slides

- Computer Security: Principles and Practice
  - Third edition, by William Stallings and Lawrie Brown
  - Schedule and lecture slides indicate next topic
    - Required to read material prior to lecture
- Lecture Slides are most important for exams
  - Posted online
  - Adapted from slides by Lawrie Brown

Chapter 1
Security Overview

Overview

Computer Security: protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).
Key Security Concepts - CIA Triad

Security Objectives

• Confidentiality
  – Prevent / detect / deter improper disclosure of information
• Integrity
  – Prevent / detect / deter improper modification of information
• Availability
  – Prevent / detect / deter improper denial of access to services provided by a system

Some Examples

• An employee should not know the salary of the manager (confidentiality)
• An employee should not be able to update own salary record (integrity)
• Salary slips should be printed on the last day of the month (availability)
More Interesting Example

• You are the security admin of a company. One day you notice that an employee is downloading a very big file. You notice that downloading a file is not exactly against company policy. Should you flag this as a security issue?

An Even More Interesting Example

You upload some financial documents on Microsoft Cloud. Microsoft analyzes these documents and determine that you owe back taxes to the IRS .....
More Security Objectives

• Authenticity – The property of being genuine and being able to be verified and trusted
  – Note similarity with integrity

• Accountability – Requirement that actions of an entity should be traceable to that entity
  – Acts as deterrence

• Non-repudiation – Requirement that an entity is not able to deny or reject the validity of its past action
  – Needed for proper accountability

Levels of Impact

Low
The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate
The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

High
The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Computer Security Challenges

1. Not simple
2. Must consider potential attacks
3. Procedures used counter-intuitive
4. Involve algorithms and secret info
5. Must decide where to deploy mechanisms
6. Battle of wits between attacker / admin
7. Not perceived on benefit until fails
8. Requires regular monitoring
9. Too often an after-thought
10. Regarded as impediment to using system
Adversary (threat agent): An entity that attacks, or is a threat to, a system.

Attack: An assault on system security that derives from an intelligent threat that is, an intelligent set that is a deliberate attempt (especially in the sense of a method or technique) to exploit security services and violate the security policy of a system.

Countermeasure: An active, defensive, preventive, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk: An estimation of how expressed the probability that a potential threat will exploit a particular vulnerability with a particular harmful result.

Security Policy: A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset): Data contained in an information system or a service provided by a system, or a system capability, such as processing power or communication bandwidth, or an entire computer system that is vulnerable to unauthorized access (hardware, software, documentation), or a facility that houses system operations and equipment.

Threat: A potential or real violation of security, which exists when there is a circumstance, especially an action or event, that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

---

Systems Security Components / Terminology

---

Assets of a Computer System

- Hardware
- Software
- Data
- Communication facilities and networks
Vulnerabilities, Threats and Attacks

- System resource vulnerabilities
  - Be corrupted (loss of integrity)
  - Become leaky (loss of confidentiality)
  - Become unavailable (loss of availability)
- Attacks are threats carried out and may be
  - Passive
  - Active
  - Insider
  - Outsider

Attacks

- Classified as passive or active
- Passive attacks are eavesdropping
  - Release of message contents
  - Traffic analysis
  - Are hard to detect so aim to prevent
- Active attacks modify/fake data
  - Masquerade
  - Replay
  - Modification
  - Denial of service
  - Hard to prevent so aim to detect

Achieving Security

- Security Policy
  - What needs to be secured?
- Security Mechanisms (Countermeasures)
  - How can it be secured?
  - Prevention, detection, deterrence, response, recovery
- Security Evaluation
  - Has the system been secured?
- Assurance
  - How well has it been secured?
Countermeasures

- Means used to deal with security attacks
  - Prevent
  - Detect
  - Deter
  - Recover
- May result in new vulnerabilities
- May have residual vulnerability
- Goal is to minimize risk given constraints

<table>
<thead>
<tr>
<th>Threat Consequences</th>
<th>Threat Action (Attack)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Disclosure</td>
<td>Exposing sensitive data directly released to unauthorized entity.</td>
</tr>
<tr>
<td>Unauthorized Access to Data</td>
<td>Unintentionally allowing unauthorized entity access to data indirectly acquired from data traveling between authorized sources and destinations.</td>
</tr>
<tr>
<td>Misuse</td>
<td>Malicious actions taken by an authorized entity.</td>
</tr>
<tr>
<td>Disruption</td>
<td>Prevents or impairs system operation by halting a system component or function.</td>
</tr>
<tr>
<td>Deception</td>
<td>Causes a system component to perform a function or service that is detrimental to system security.</td>
</tr>
</tbody>
</table>

**Table is on page 20 in the textbook.**

Computer and Network Assets, with Examples of Threats

<table>
<thead>
<tr>
<th>Availability</th>
<th>Confidentiality</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Equipment is stolen or disabled, thus denying service.</td>
<td>An unencrypted CD-ROM or DVD is stolen.</td>
</tr>
<tr>
<td>Software</td>
<td>Programs are deleted, denying access to users.</td>
<td>An unauthorized copy of software is made.</td>
</tr>
<tr>
<td>Data</td>
<td>Files are deleted, denying access to users.</td>
<td>An unauthorized read of data is performed.</td>
</tr>
<tr>
<td>Communication Lines and Networks</td>
<td>Messages are destroyed or deleted.</td>
<td>Messages are read. The traffic pattern of messages is observed.</td>
</tr>
</tbody>
</table>

Threat Consequences and the Types of Threat Actions That Cause Each Consequence

Based on RFC 4949
Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:
- Open ports on a host or device, and allow incoming and outgoing data
- Port is open and available on the outside of a firewall
- Code that processes email, office documents, and various specific exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to a vulnerable system is vulnerable to a social engineering attack

Attack Surface Categories

- Network Attack Surface
- Software Attack Surface
- Human Attack Surface
Security by Obscurity

- If we hide the inner workings of a system, it will be secure
- Bad idea
  - Less and less applicable in the emerging world of vendor independent open standards
  - Less and less applicable in a world of widespread computer knowledge and expertise

Security by Legislation

- If we instruct our users on how to behave, we can secure a system
- Bad idea
  - User awareness and cooperation is important but cannot be the principal focus for achieving security
  - Human beings tend to defy authority
Weakest Link In Computer Security

- Human beings are often considered the weakest link
  - 95% of all attacks were directed against the home computer user in 2007
  - End-users are frequently exposed to security risks through routine on-line activities such as checking email or web browsing
  - Many recent attacks indicate that end-users are increasingly becoming a new form of threat in cyber-space, the so-called *unwitting accomplice*

What’s Next

- Read rest of Chapter 1
  - Lot's of terminology; refer to slides for more important ones
  - Focus on big picture and recurring concepts
- Start reading Chapter 2
- Expect receiving email in your rams.colostate.edu address about account creation on DETER network
  - Follow instructions in email to complete account creation process.