Engineering Secure Software

COURSE OVERVIEW

Vulnerability of the Day

- Each day, we will cover a different type of code-level vulnerability
  - Usually a demo
  - How to avoid, detect, and mitigate the issue
- Most will link to the Common Weakness Enumeration
  - http://cwe.mitre.org

In-Class Activities

- Most days, we will cover a tool or technique
- Many activities are interactive and collaborative in nature
  - …so attendance is necessary
- Activities are for learning
  - Formative feedback, not summative
  - No submissions (usually) – instructor checks in class
  - Exams will have questions about those activities

Exams

- Midterm & Final exam

- Closed book
- Closed computer
- Covers lecture material, VotD, textbook, and activities

Case Study

- Choose a large software project to study
  - Source code must be available (>10k SLOC)
  - Domain must have security risks
  - History of vulnerabilities must be available
  - Instructor approved
- Paper with chapters on:
  - Security risks of the domain
  - Design risks
  - Code inspection results
- Iterative paper writing
  - Multiple submissions over the quarter
  - You are graded on the content and how you react to my feedback

Case Study Ideas

- Tomcat
- MySQL
- PostGreSQL
- Linux kernel
- PHP
- Ruby
- Ruby on Rails
- Hibernate
- Wireshark
- Wordpress
- Firefox
- Chromium
- Drupal
- MediaWiki
- Apache httpd
- Android
- Java
- X Windows
- Gnome
- KDE
- Thunderbird
- PHPMyAdmin
- RT
- Django
- OpenSSL
- VLC
- Samba
- Quagga
- Joomla
- GLibC
- OpenMRS
- Pidgin

Fuzz Testing Project

- We will have one larger programming project
  - Building a tool for automated security testing
  - More info to be announced later

For Next Time

- Get into groups of 3 for the case study
  - If need be, we can have one or two pairs
- Use your GoogleDocs@RIT account
  - Create a *Collection* named “SE331 X” where X is your case study
    (you can rename it if you change)
  - Add **andy.meneely@gmail.com** as an editor
- Due 2-1
  - Case study proposal (see website)