CS 161: Computer Security

Lecture 0

August 27, 2015

Course staff

- Doug Tygar, instructor
- David Fifield, volunteer
- Robin Hu, TA
- Bill Yeh, TA
- Qi Zhong, TA
- Lynn Tsai, Reader
- Barbara Goto, Assistant to Doug Tygar

Lectures and sections

- Lecture Tuesday & Thursday 3:30-5:00
- Section on Wednesday
  - 10-11 (Bill Yeh)
  - 11-12 (Qi Zhong)
  - 12-1 (Qi Zhong)
  - 1-2 (Bill Yeh)
  - 2-3 (Robin Hu)
  - 3-4 (Robin Hu)

Office Hours

- Monday
  - 11AM – Doug Tygar (location TBA)
  - 3PM – Robin Hu (Soda 611 alcove)
  - 5PM – Bill Yeh (Soda 411 alcove)
- Thursday
  - 11AM – David Fifield (Soda 723)
- Friday
  - 2PM – Qi Zhong (location TBA)

- Anytime by appointment ….

Waitlist

- We have seats available in class
- Need to find an available section
  - You need to attend section, so this is important!

- Concurrent enrollment – looks good
  - But will not be processed until next week at earliest

Piazza

- This class is based on Piazza
- All hand-outs, notes, etc. will be on Piazza
  - (or linked from Piazza)
  - Notes are available after lecture (not before lecture)
- You are responsible for regularly monitoring Piazza
- Fun fact: Instructors get detailed analytics on Piazza
  - Broken down by student: how often you read Piazza, how often you post, etc.

Class syllabus (high-level)

- September 1 - 29: Cryptography
- October 1: Midterm 1
- October 5 - 27: Network Security
- October 29: Midterm 2
- November 2 – December 1: System Security
- December 3: Midterm 3

Midterms are in-class, closed book, cumulative.

(Likely will allow a “cheat-sheet” of notes – check later)

No class or section on November 24-25 (before Thanksgiving)

No final

Handwriting is important

- If we cannot read your answer, we cannot grade your midterms

- If you have a disability issue with writing, please check with DSP office for assistance.

Prerequisites

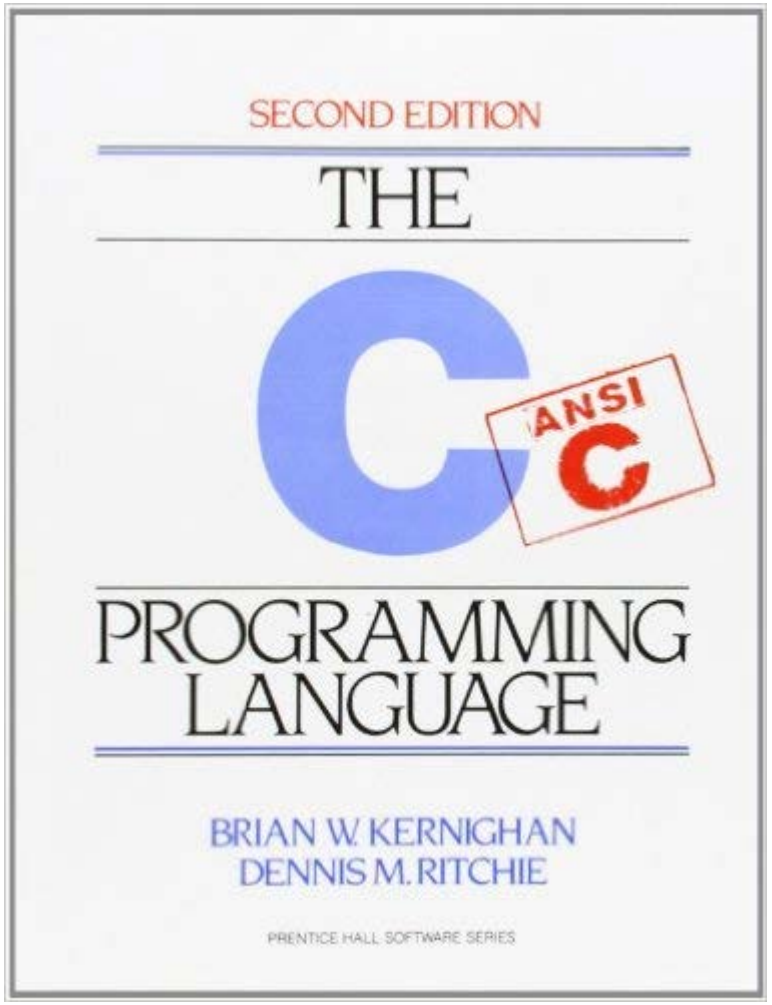
- CS 61C
  - C programming
  - Assembly programming
  - Basic architecture
    - Special registers: Stack pointer, frame pointer
- CS 70
  - RSA
  - Shamir secret sharing
  - Modular arithmetic
    - Special case – modulo prime (finite field)
  - Chinese remainder theorem (if you studied)

Textbooks

- No required textbooks
- We have six (!!) recommended textbooks

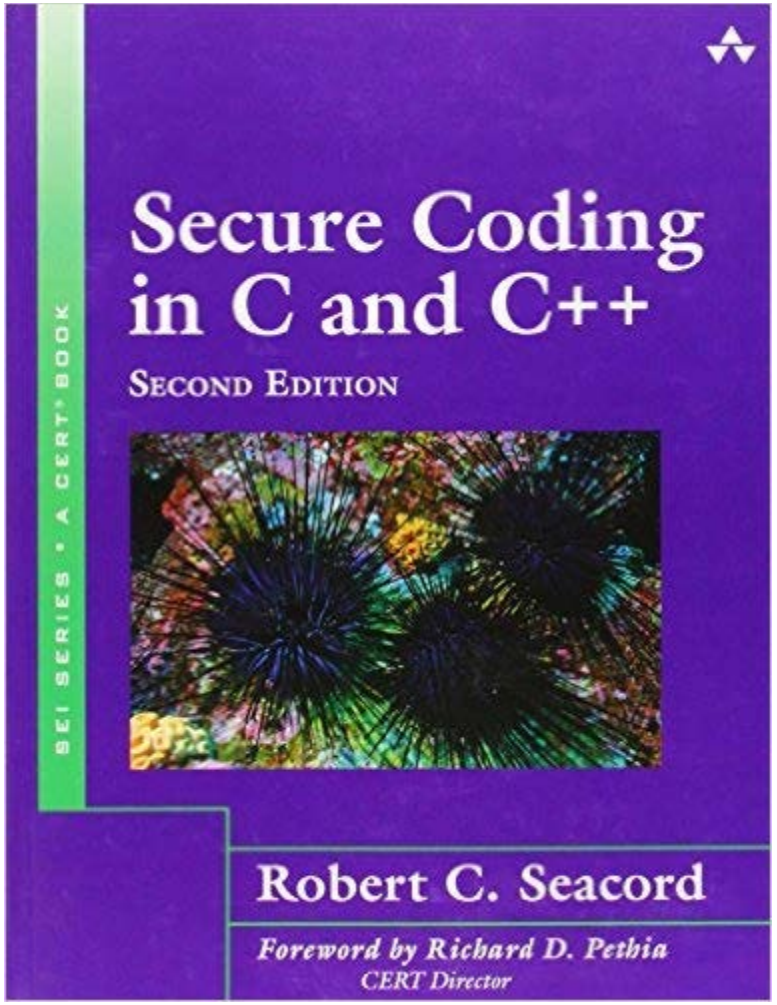
C Programming Language 2nd ed

- Systems programming
- ISBN 978-0131103627



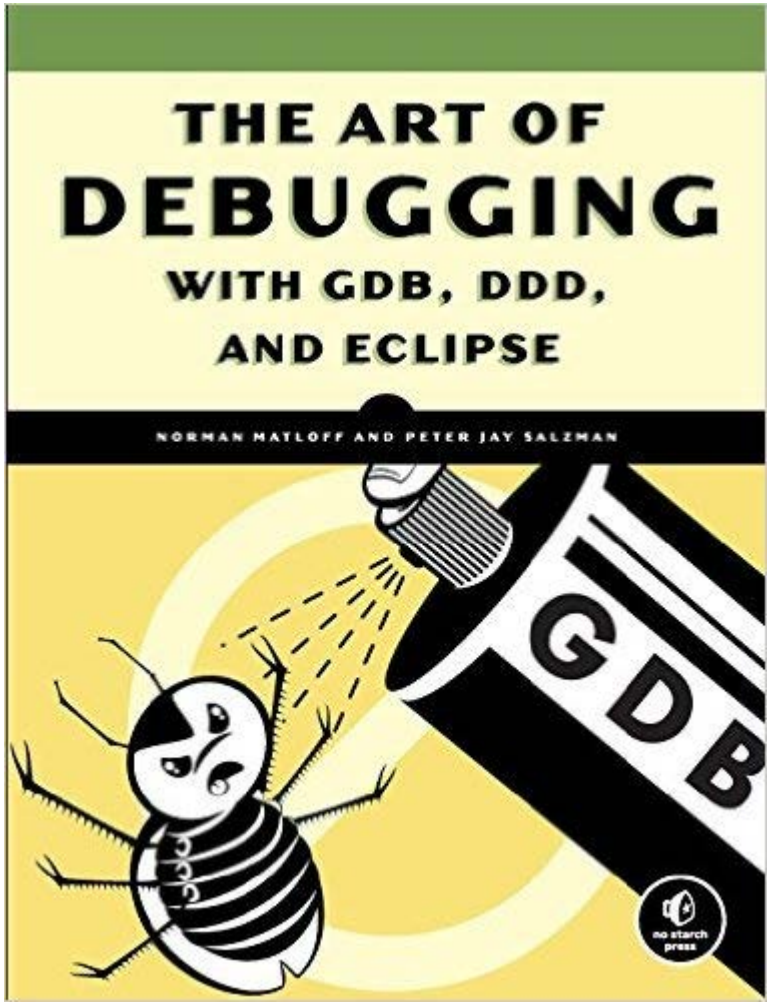
Secure Coding in C and C++ 2nd ed

- Systems programming
- ISBN 978-0321822130



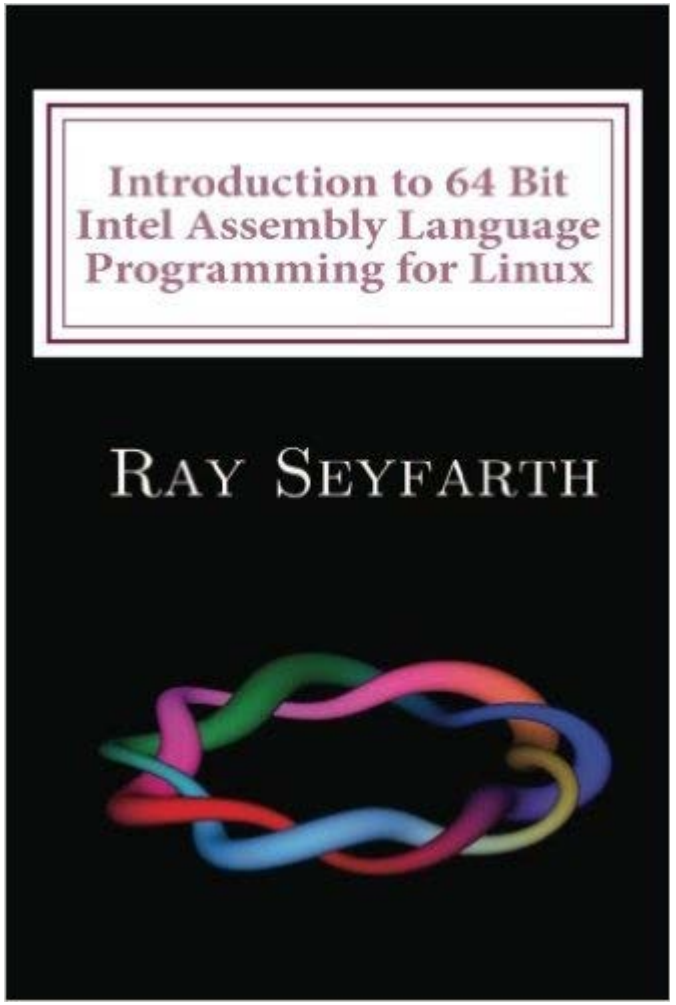
Art of Debugging with GDB …

- You need to debug C
  … and assembly
- ISBN 978-0321822130



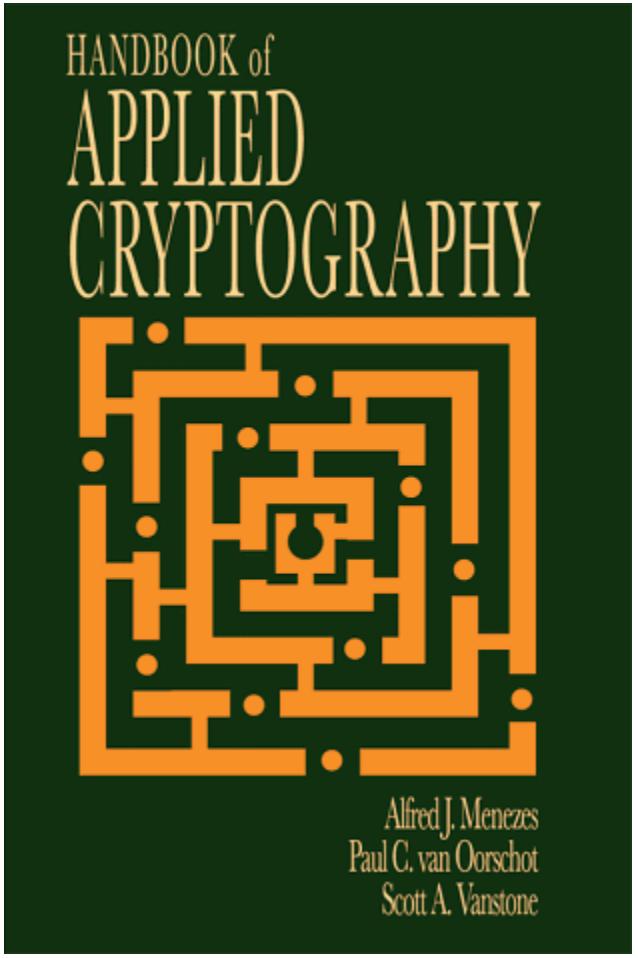
Intro to 64 Bit Intel Assembly ...

- Introduction to x86-64
- ISBN 978-1478119203



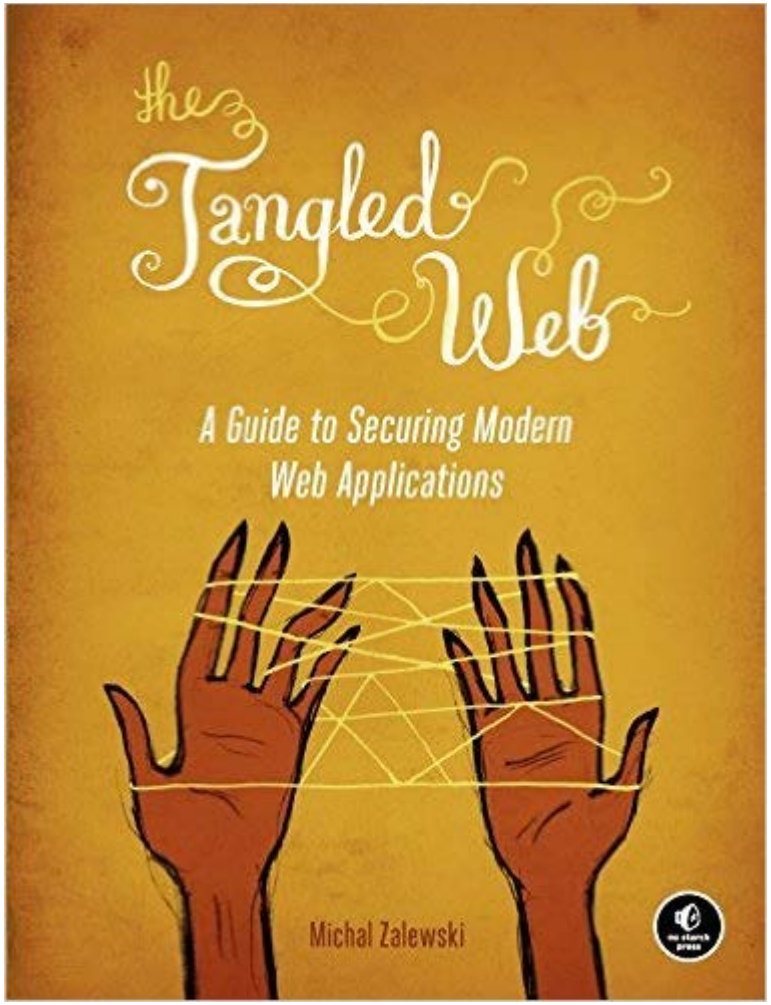
Handbook of Applied Cryptography

- Basic crypto reference
- Free online version
- ISBN 978-8189836122



The Tangled Web

- Web security
- ISBN 978-1593273880



Homework

- We will generally have homework weekly
- Due on Tuesdays at 3PM
- Gradescope (written homework)
- glookup (programming)
- Late homeworks not accepted

- Note: hive is flakey.
  - Prepare for downtime
  - Will *consider* extensions if down more than 6 hours

Crunch time

- Crunch time will be first week of December
  - Midterm 3
  - Likely project due date
  - Likely homework due date
- Plan ahead for this tsunami

Grading

- 35% Midterms
- 25% Project
- 20% Homework
- 20% Class & Section participation

- EECS Policy on grading:
  - http://bit.ly/eecs-grading

- No incompletes; no late materials

If you want an “A” or “A-”

- You should do well on *all* class components
- You should help out with class
  - Example: answering questions on Piazza
  - Helpful Piazza answers impress the instructors!

Regrade requests

- Make regrade requests via gradescope
  - Or, for programming, to your TA
- Don’t send them to Doug (unless he graded the question)
- Frivolous regrade requests may result in suspending regrading privileges

All in

- You are paying a lot of tuition
- No point in just “dabbling” in CS 161
- Go all in:
  - Attend all classes
  - Attend all sections
  - Participate in piazza
  - Don’t use electronics in class (except to take notes, look up references)
  - Engage!

Missing class

- Good excuses (we may ask for verification)
  - Emergency
  - Religious holidays
  - Scientific conference
  - Health issues

- Not so good excuses
  - Oversleeping (the class starts at 3:30, dude!)
  - Scheduling romantic dates during class
  - Hangovers
  - Interviews (don’t schedule during class!)

Easy ways to flunk CS 161

- Have electronics make noise in class
  - Take a phone call in class
- Tweet, Facebook, Instagram, etc during class
  - This includes posting on Piazza in class
- Regularly miss class or section
- Copy homework/projects/etc

Intellectual honesty

- Cite all sources you use
- Do all homework on your own
  - Copying, cheating → failure in course
  - Referral to Office of Student Conduct
  - http://bit.ly/eecs-dishonesty
  - If there is a question, ask an instructor
- Don’t cheat on midterms
  - See above!

Disabled?

- Disabled & require special accommodations?
  - Have Disabled Students Program (DSP) send letter
  - Letter should be sent right away – otherwise we will not be able to schedule disabled proctoring
  - DSP requires long lead times to schedule proctoring
  - Work with DSP to schedule proctoring a week before exams

Frequently asked questions

Section

- Q: Can I go to a different section?
- A: For next week or two, no.
  After then, you can switch sections as long as there is room and you get permission from both old and new TAs.

- Q: Can I go to more than one section?
- A: Yes, as long as there is room in the additional section

Programming

- Q: Can we use Java instead?
- A: No. C and Assembly are standard for systems programming

- Q: Can we use Go or C++ or …
- A: No. We are set up to support C and Assembly in this class

Webcasting

- Q: Will the course be webcast?
- A: No.

  Good video requires different preparation

  Poor results when students rely on webcasts

- Q: May I record lectures?
- A: Only if you have permission from DSP office

Incompletes

- Q: I saw that you don't give incompletes, but I have a good reason. What can I do?

- A: It is as easy to process a grade change form as an incomplete.

  We'll give you a preliminary grade based work to date, and after emergency is over, can discuss if we should change grade.

Hints

- Q: I am having problems with the homework. Can I have a hint?
- A: No, but we can discuss the underlying material we covered in lecture.

- Q: Can I post hints on Piazza, or ask “is this answer correct?”
- A: Please don’t – we consider that cheating

Programming help

- Q: My C program doesn't work. Can you explain what I did wrong?
- A: No, but we can help you get started with GDB

- Q: What does "bus error" (or "segmentation fault" mean)?
- A: It means you need to use GDB

Computer security

- Relevant, useful, makes you highly employable
- Course allows good integration of both systems & theory
- My goal: cover lots of ground & keep course fun