Computing and Society I



Admin



- Questions?
- Quizzes return Nov 23-25

Course outcomes



- Let’s look at the syllabus for the course outcomes

Course outcomes



- Let’s look at the syllabus for the course outcomes
  - We’ve covered most of them.
  - But some completely untouched
    - Recursion
    - Simple algos incomplete
    - Functions from fundamental syntax
    - Computers and Society
  - So let’s fix that – at least for one of them
- Oh and yes – it is on the outcomes, so it will be on the quizzes/exams

Ethics and Responsibility



- In Math/Science discipline like computer science
  - easy to focus on getting the program right
  - but also need to consider the program itself.
  - In age of computerized everything
    - do we really want all functions computerized.
    - for those that are, what are the risks
    - What are the (unintended) consequences?

The rent Algorithm



- A company (RealPage) created an algorithm to help landlords set rents to the maximum amount the market would bear.
- https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent
- In the old days
  - Want to see if you should raise rent? Call around pretending to be a potential renter.
  - Now plug your apartments into the rent algorithm like so many others and it will tell you.
  - The money quote: “One of the algorithm’s developers told ProPublica that leasing agents had “too much empathy” compared to computer generated pricing.”

The Rent algorithm update

- Everyone thinks this is terrible
  - In a rare moment of bi-partisanship, a lawsuit filed in the very end of the Biden administration in late 2024, was settled by the Trump administration in late 2025 forcing RealPage to stop price-fixing
  - https://www.propublica.org/article/doj-realpage-settlement-rental-price-fixing-case
  - Buuut……..

The Rent algorithm update

- Everyone thinks this is terrible
  - In a rare moment of bi-partisanship, a lawsuit filed in the very end of the Biden administration in late 2024, was settled by the Trump administration in late 2025 forcing RealPage to stop price-fixing
  - https://www.propublica.org/article/doj-realpage-settlement-rental-price-fixing-case
  - Buuut…… a new company stepped in to try to take over the space: WillowBridge
  - So a new Settlement in summer 2026
  - https://www.duanemorris.com/alerts/dojs_proposed_settlement_property_manager_targets_pricing_coordination_rental_housing_0726.html
  - And apparently now some are preemptively counter suing
  - https://www.multifamilydive.com/news/algorithmic-rent-pricing-lawsuit-tracker/826178/

Ethics and legality



- This is not always easy – because unethical and illegal are not always the same
  - https://medium.com/free-code-camp/the-code-im-still-ashamed-of-e4c021dff55e
  - Summary: young man gets good job building software quiz for drug company that pushed company's drug
  - Quiz site is aimed at teen-aged girls
    - Company's drugs most common side effects were guess what?

Ethics and legality



- This is not always easy – because unethical and illegal are not always the same
  - https://www.freecodecamp.org/news/the-code-im-still-ashamed-of-e4c021dff55e
  - Summary: young man gets good job building software quiz for drug company that pushed company's drug
  - Quiz site is aimed at teenaged girls
    - Company's drugs most common side effects were guess what?
    - "It turned out that among the main side effects of that drug were severe depression and suicidal thoughts."
- Tell Story of a middle aged students blackballed from industry and he had to move here

Bugs



- computer complexity
  - bugs a fact of life
  - MS windows
    - Monthly updates - > irregular updates.
  - Linux& unix (including Mac)
    - irregular updates.
  - Steam
    - Games and apps, update required?
  - live with bugs in some things
    - but not others.
    - like what?

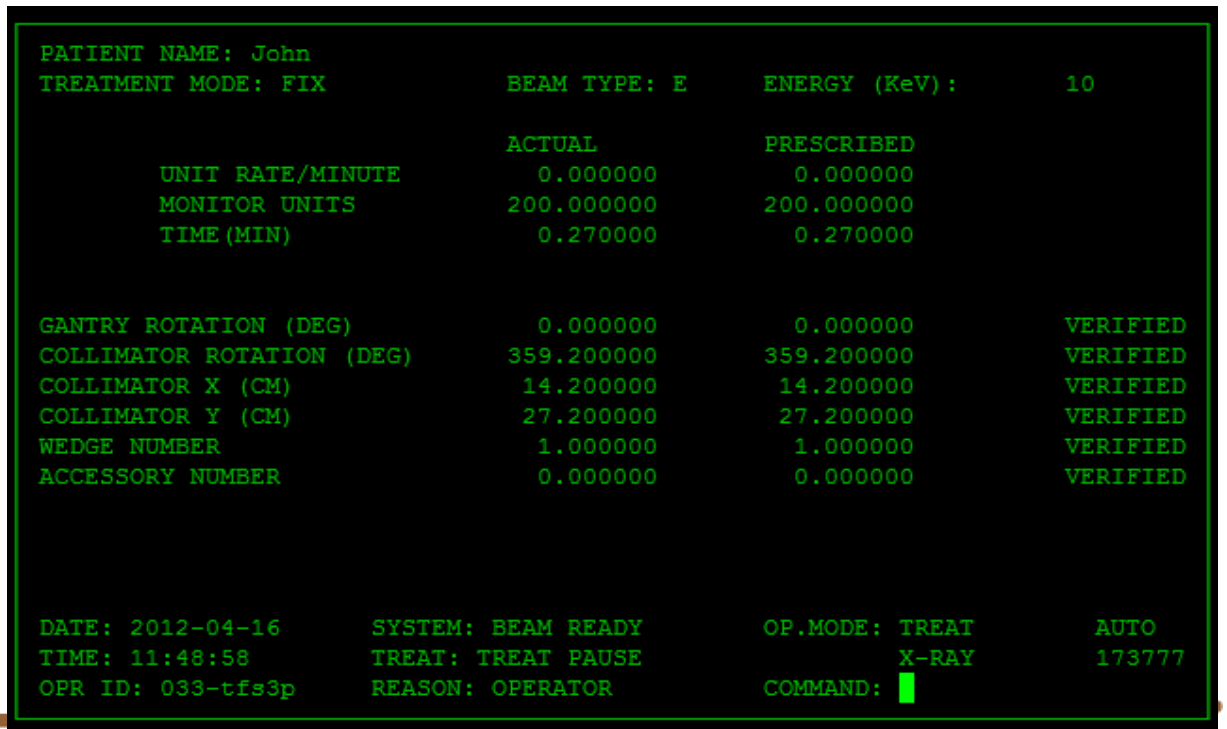
Therac-25: The first software assisted Deaths



- Therac-25 total computer problem.
  - radiation treatment machine
  - successor to previous machines developed as joint venture.
  - completely software controlled.
    - previous versions of software designed for previous machines
    - prev machines had hardware safeties.
    - operator types x (x-ray), then e (low powered electron beam), system reports ready, operator says go
      - system says error (usually means dose not administered)
      - operator tells it to try again.

Therac-25 Interface

- https://upload.wikimedia.org/wikipedia/commons/9/90/Therac25_Interface.png
-



But the Therac-25 was a long time ago



- Therac-25 was a story about
  - how a company fundamentally changed a hardware product which looked to its users like the same product
  - The company used (buggy) software to try to bridge the gap.
  - And that was a long time ago – every (ABET accredited or ACM compliant) CS program covers this, so we learned our lesson right?

But the Therac-25 was a long time ago



- Therac-25 was a story about
  - how a company fundamentally changed a hardware product which looked to its users like the same product
  - The company used (buggy) software to try to bridge the gap.
  - And that was a long time ago – every (ABET accredited or ACM compliant) CS program covers this, so we learned our lesson right?
  - Then why does that story sound familiar to us today?
  - Think of a problem from about 7 years ago?
    - Different hardware – ‘papered over’ with software leading to death and disaster?
    - In aviation this time

But the Therac-25 was a long time ago



- Therac-25 was a story about
  - how a company fundamentally changed a hardware product which looked to its users like the same product
  - The company used (buggy) software to try to bridge the gap.
  - Why should that sound familiar to us today?
    - Boeing 737 Max

Boeing 737 Max



- Boeing 737
  - Entered airline service 50+ years ago in 1968
  - Has been a workhorse ever since
- Boeing 737 Max
  - Entered airline service in 2017
  - Looks like a 737 in many ways (body is the same)
  - Much bigger engines - Flies completely differently
  - Has computer assist flying
    - Really doesn’t like to give pilots control when a sensor fails.
  - Fatal software assisted crashes in 2018 and 2019
- Same fundamental problem 35 years later

British Postal Scandal



- British postal software led to wrongful prosecution of at least 1000 people over at least 13 years
  - And likely more than 10,000 were improperly fined.
  - https://archive.md/20250711010254/https://www.nytimes.com/2025/07/10/world/europe/uk-post-office-scandal-report.html
  - Described as one of the worst miscarriages of justice in British history
  - Software rolled out in 1999 (alleged that software devs knew of problems then)
  - By 2000 first “problems balancing the books” reported.
    - Postal service tells each postmaster/assistant complaining that “they are the only one”
  - By 2013 Members of Parliament start investigating
  - In 2020 a formal investigation starts
  - In 2025, 166 page report of damming evidence implicates developers at the software shop and Postal management for destroying lives (including at least 13 suicides)
  -

Software Disasters with CS1 Understandable Causes



- 1991: Early Patriot Missile Failure
- 1996: ESA loses rocket
  - http://www.ima.umn.edu/~arnold/disasters/ariane.html
- 1998: NASA Mars orbiter fails – crashes into mars http://www.jpl.nasa.gov/news/releases/99/mcoloss1.html
- 2016 internet outage in much of east coast US
- Some of these are pretty old, but not as old as the Therac-25 when Boeing managed to repeat history

Patriot Missal Failure



- 1991 Gulf war I
  - summary: Patriot Missile battery in Dharan, Saudi Arabia, failed to track and intercept incoming Iraqi Scud missile. Scud struck an Army barracks, killing 28 soldiers and injuring around 100 other people
  - cause: small rounding error caused by representing fraction 1/10 in binary (repeating number in binary)
    - hardware had counter that counted number of tenths of a second since bootup. Get current time by counter * 1/10
    - time needed to predict where scud should be at current time.
    - battery had been on alert for 100 hours, error was .34 seconds
      - in that time the scud traveled close to half a mile.

ESA Loses Rocket



- On June 4, 1996:
  - unmanned Ariane 5 rocket launched by the European Space Agency exploded just forty seconds after its lift-off
  - rocket on its first voyage,
  - cost:
    - a decade of development costing $7 billion.
    - rocket and its cargo valued at $500 million.
- cause of the failure
  - software failure
  - 64 bit floating point number relating to the horizontal velocity of the rocket was converted to a 16 bit signed integer
  - value was greater than32,767
  - Python just makes a bigger type of number, but that is why it is too slow for rocket science

Mars Orbiter Crashes



- Units Units Units
  - Mars Orbiter crashes
  - Cause: two teams, two states, two sets of units
    - California team: This is NASA, we are in the United States, of course we are using feet and pounds
    - Colorado team: This is science, of course we are using newtons and meters
  - As you know, when passing and argument to a function, no units attached – just a number
  - So splat.

2016 Internet outage in Eastern US



- 2016 internet in much of eastern US down for afternoon
  - Cause, thousands of compromised IoT devices used to DDOS the name servers
    - DDOS?

2016 Internet outage in Eastern US



- 2016 internet in much of eastern US down for afternoon
  - Cause, thousands of compromised IoT devices used to DDOS the name servers
    - DDOS? Distributed Denial of Service attack
    - Basically they were asking “what is the number for this server?” so much that the name servers couldn’t keep up.
  - Root cause: tens of thousands of small devices like ring doorbells and internet enabled fridges that had never changed the default password and got ‘hacked’
- Fix since then: don’t let customers use all the features of their devices till they change the passwords.

Small selection



- Small selection of major software and human interaction glitches
  - some worse than others
  - Some cherry-picked to be understandable by CS1 students
  - some situations need to be more careful than others.
  - Many are from a while ago.
    - software better?
    - maybe just more declassified from a while ago.
    - Look at the generator blow up – the demo happened in 2007 but it wasn’t made public till 2020
- And of course next

Log4j (log4shell)



- Log4j
  - Small open source logging library for java
  - Maintained by 3 unpaid volunteers in their spare time
- Dec 2021, vulnerability discovered as Minecraft server hack
  - Discuss logging
    - Deeper look for those interested: https://news.sophos.com/en-us/2021/12/17/inside-the-code-how-the-log4shell-exploit-works/
  - What could go wrong?

Log4j (log4shell)



- Log4j
  - Small open source logging library for java
  - Maintained by 3 unpaid volunteers in their spare time
- Dec 2021, vulnerability discovered as minecraft server hack
  - Discuss logging
    - Deeper look for those interested: https://news.sophos.com/en-us/2021/12/17/inside-the-code-how-the-log4shell-exploit-works/
  - What could go wrong?
    - https://www.express.co.uk/life-style/science-technology/1539451/log4j-vulnerability-empty-victims-bank-accounts
    - https://www.politico.eu/article/belgium-defense-ministry-hit-with-cyberattack/
      - Belgium in Dec 2021 – what happened 2-3 months later?

Chase Bank ‘infinite money glitch’



- Aug-Sept 2024 chase bank ATMs are vulnerable to check fraud
  - Failure of Software Engineers (CS) and Software Security Professionals (Cyber)
  - ATMs accepts fraudulent checks, don’t contact the issuing bank to make sure the funds exist, and then immediately make cash available to dispense
  - https://www.yahoo.com/news/chase-says-viral-bank-glitch-trend-is-actually-fraud-a-cybersecurity-expert-explains-why-financial-hacks-that-seem-too-good-to-be-true-usually-are-213629242.html

Shai-Hulud Malware on ctrl/TinyColor



- In Sept 2025 we had the Shai-Hald (sha1-hulud) Malware attack
  - Lets get one of the cyber security folks to tell us what happened
    - Since it was a few weeks ago.

Shai-Halud Malware on ctrl/TinyColor



- In Sept 2025 we had the Shai-Halud Malware attack
  - A contributor to a npm (the main javascript/web programming package manager) package had access to a github repository with a *secret* token to publish several packages to NPM.
  - The contributor used this to publish a corrupted version of TinyColor (2million downloads a week) and about 40 lesser used npm packages.
  - When installed as part of a web developer's toolchain, these infected packages would scan the local machine for more secrets and push them to a remote website.
  - The whole thing was an issue for a bout 12-24 hours. The extent of the lost secrets/tokens is unclear as of Sept 17 2025

Cyber Security and SBOMS



- What are SBOMs
  - Especially you cybersec folks
  - Though you haven’t met them formally in courses yet

Cyber Security and SBOMS



- What are SBOMs
  - Software Bill Of Materials
  - Most Cyber Security (And many of the Software Engineers who work with them and have them embedded in their software dev teams) will work with them
  - Basically a list of all of the ‘dependencies’ (external libraries like DearPyGui and friends) and dependencies of those dependencies in the software being developed.
- Most cyber sec folks will likely need to know multiple programming languages including scripting and ‘infrastructure as code’ langauges. (this compromise was github actions – infra as code)
  - Software devs might just know 2-4 languages really deeply.

Security and Big numbers



- A lot of the internet is secured by big numbers
  - If finding those big numbers is expensive security is pretty good.
  - Tell me about factoring of a number
    - Yup you can never forget your grade school math.
    - Lucky Volunteer?™

Security and Big numbers



- A lot of the internet is secured by big numbers
  - If finding those big numbers is expensive security is pretty good.
  - Tell me about factoring of a number
    - Finding the numbers you have to multiply together to get the original number
    - Eg: 24 → 3x8 or 12x2 or 6x4
  - Disclaimer: below is simplification, cyber folks can learn more in upper level courses
    - A lot of current cryptography is based on the idea that it is easy to multiply the two numbers together when you know them, but hard if all you have is the original number and you have to find the correct factors.
    - Especially when the numbers are large.

Security and Big Numbers II



- The ‘cryptographic keys’ are these big numbers
- How big do you suppose?
    - Lucky Volunteer?™

Security and Big Numbers II



- The ‘cryptographic keys’ are these big numbers
- How big do you suppose?
  - Usually about 116 digits long.
- How should we generate these numbers?
  - “How about we select a random number from zero to the digit 9 116 times in a row?” -eMudhra, cryptographic provider
  - What could *possibly* go wrong?

Security and Big Numbers II



- The ‘cryptographic keys’ are these big numbers
- How big do you suppose?
  - Usually about 116 digits long.
- How should we generate these numbers?
  - “How about we select a random number from zero to the digit 9 116 times in a row?” -eMudhra, cryptographic provider
  - What could *possibly* go wrong?
  - In October 2026, it was discovered that one of the generated keys was 4
    - (and several other 2 and 3 digit keys)
    - Cryptography broken in milliseconds – no quantum needed.

But AI will save us right?



- AI will save us
- https://www.technologyreview.com/2023/02/20/1068824/ai-actually-helpful-disaster-response-turkey-syria-earthquake/
- Really bright people say so
- https://a16z.com/ai-will-save-the-world/
-

But AI will save us right?



- What happens when AI starts reporting something that isn't true
- https://www.firstpost.com/world/chatgpt-makes-up-a-sexual-harassment-scandal-names-real-professor-as-accused-12418552.html
- Or they start trying to learn from each others output
- https://www.businessinsider.com/ais-trained-on-each-other-start-produce-junk-content-study-2023-6
- These AIs are amazing tools - as long as you use them as tools, if you let them drive, they are not
  - https://www.pcmag.com/news/vibe-coding-fiasco-replite-ai-agent-goes-rogue-deletes-company-database
- Which is why you need to know this (comp151) material deep in your bones, so you can **use** it well, rather than letting it run the show

Fable/Mythos



- Mythos
  - Was so ‘dangerous’ it had to be restricted for a couple of weeks in early 2026
  - Founds lots of undisclosed bugs
  - https://www.endorlabs.com/learn/what-is-mythos-and-why-it-matters-for-software-security
  - I heard a talk from a senior tech manager who had been a dev and was in industry for 25 years
    - He ran Mythos on his companies code base
    - What did it find?

Fable/Mythos



- Mythos
  - I heard a talk from a senior tech manager who had been a dev and was in industry for 25 years
    - He ran Mythos on his companies code base
    - What did it find? : around 400 ‘vulnerabilities’
    - As a tech savvy person he looked at the results and found that 300 were complete non-sense, another 50 or so were so minor it would have been a complete waste of time to have any of his people work on them
    - Under 50 needed anyone to look closely at them.
  - Theme of the course: tools are only valuable if you know how to use them
    - Understanding what they are telling you, and ignoring all of the many junk things they tell you.

The Tea App



- The Tea App (July 2025):
  - Supposedly an app where women can share stories about abusive partners so other women will know
  - Actually: A massively insecure app coded by someone with six months of experience heavily leaning on AI tools.
  - Leaks the data (including scans of drivers licenses) of 72 thousand users.
    - Turns out the credentials needed to get that data were embedded in plain text in the application
      - Any (even junior) app developer or fourth year cyber-security student will have everything they need to do that data breach.
- More evidence: You have to use the tools – don't let them drive, even 95% right in medicine or engineering leads to death or loss
- https://www.ainvest.com/news/tea-app-data-breach-exposes-72-000-users-ai-generated-code-security-lapse-2507/

PHP2Shell



- Cyber Majors,
  - Tell me about PHP2Shell, the biggest security story of Oct 2026

PHP2Shell



- Cyber Majors,
  - Tell me about PHP2Shell, the biggest security story of Oct 2026
  - Does anyone start a new project in PHP in 2026?
    - No
  - But Drupal, Wordpress and WikiMedia
    - All written in PHP and are basis of a lot of ‘mom and pop’ websites
  - Government procurement and replacement?

PHP2Shell



- Cyber Majors,
  - Tell me about PHP2Shell, the biggest security story of Oct 2026
  - Does anyone start a new project in PHP in 2026?
    - No
  - But Drupal, Wordpress and WikiMedia
    - All written in PHP and are basis of a lot of ‘mom and pop’ websites
  - Government procurement and replacement?
    - So a lot of that in PHP written a 10-20 years ago too.
  - As of Summer 2025, almost 70% of websites had some PHP
    - https://w3techs.com/technologies/details/pl-php

PHP2Shell ‘Explained’



- The vulnerability has been in PHP for 10 years
  - But never found because it requires chaining several failures together.
  - ***Roughly***,
    - cause error,
    - make PHP crash one part – memory for that part is abandoned,
    - Other part of program reuses stale memory
    - Careful crafting of the error can cause PHP to treat the crash memory as code to run
    - Allows users to execute their code on server.
  - Multiple small vulnerabilities add up
    - AI agents try again and again using statistical analysis of earlier results to finally get code in correct corrupted memory

Good for now



- We might revisit similar issues later, but now lets get back to programming fundamentals.