15-316: Software Foundations of Security and Privacy

Introduction

Fall 2022

Course Staff

Jack Duvall

Aditi Kabra

Nuno Sabino

Failed Attempts at Security: Netflix Prize

- $1million competition to improve Netflix's recommendation system
- 100 million ratings from 500,000 users
- *"All customer identifying information has been removed; all that remains are ratings and dates … only a small sample was included, and that data was subject to perturbation"*

A brief digression

- October 1987: US Senate rejects Robert Bork's SCOTUS nomination 42-58

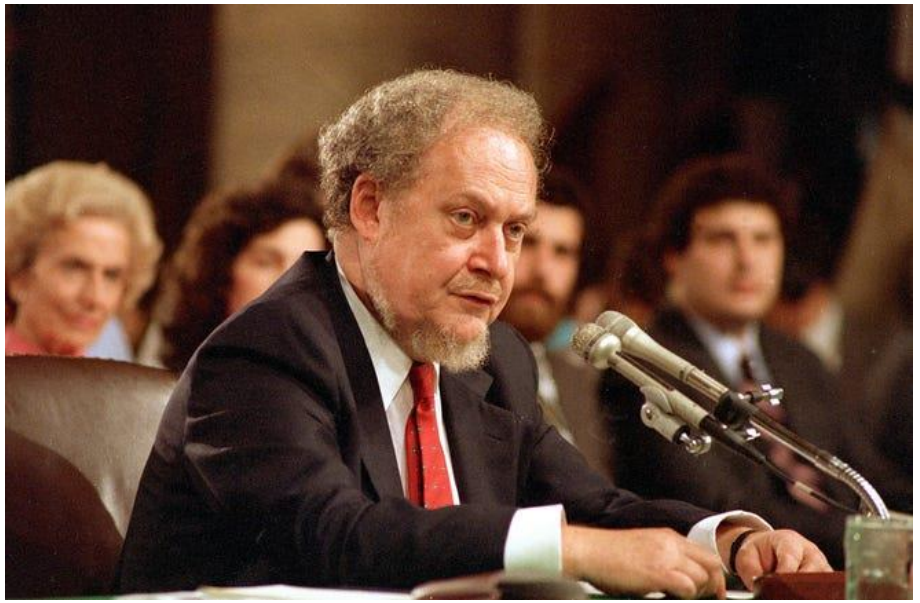


Image source: Associated Press, 1987

A brief digression

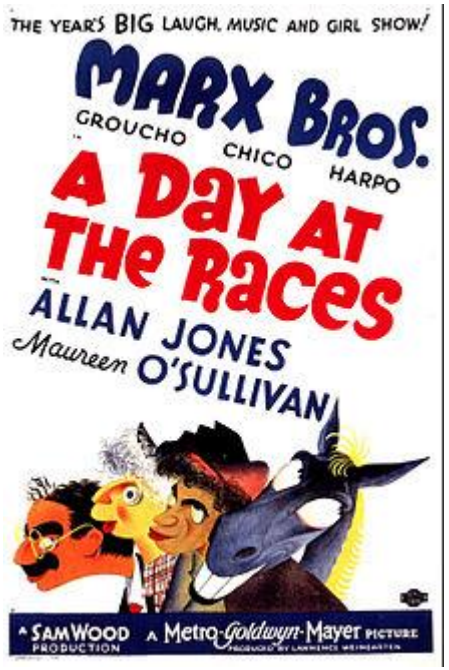
- October 1987: US Senate rejects Robert Bork's SCOTUS nomination 42-58
- Ted Kennedy, 45 minutes after Bork's nomination:

  "Robert Bork's America is a land in which women would be forced into back-alley abortions, blacks would sit at segregated lunch counters, rogue police could break down citizens' doors in midnight raids, and schoolchildren could not be taught about evolution…"

- During the debate, Bork's video rental history was leaked to the press

Image source: Associated Press, 1987

Stunning revelations



Video Privacy Protection Act of 1988

- 18 U.S. Code § 2710 –

  Wrongful disclosure of video tape rental or sale records

- ***(b)(1)*** *A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection* ***(c)****.*
- ***(c)(2)*** *The court may award—actual damages but not less than liquidated damages in an amount of $2,500; punitive damages; reasonable attorneys' fees; and such other preliminary and equitable relief as the court deems appropriate.*

Robust De-anonymization of Large Sparse Datasets

Arvind Narayanan and Vitaly Shmatikov
The University of Texas at Austin

- **Recall:** *"All customer identifying information has been removed; all that remains are ratings and dates … only a small sample was included, and that data was subject to perturbation"*

	The Godfather	12 Angry Men	Forrest Gump	…	Les Chiens	Bye Bye Monkey	Themroc	Sumo Do, Sumo Don't	Spies
User1	5	4	3	…				5	
User2	2	4	5	…	1				
User3	5	5	5	…					3

Commonly Rated

More Obscure

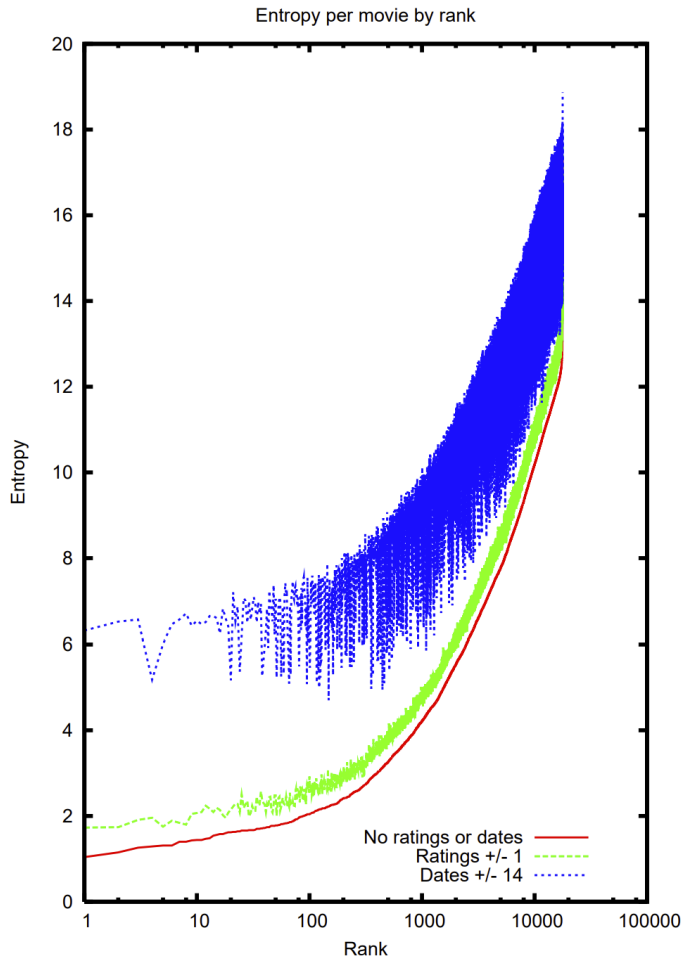
Entropy and identity

- Entropy is a measure of the uncertainty about a random outcome
- Defined as the expected negative logarithm of the probability, measured over all outcomes

  $H(X) = \mathbf{E}\,[-\log p(X)\,]$
- *Without any prior information about the outcome, how many bits do we need to uniquely identify a randomly-selected…*
  - person on earth?

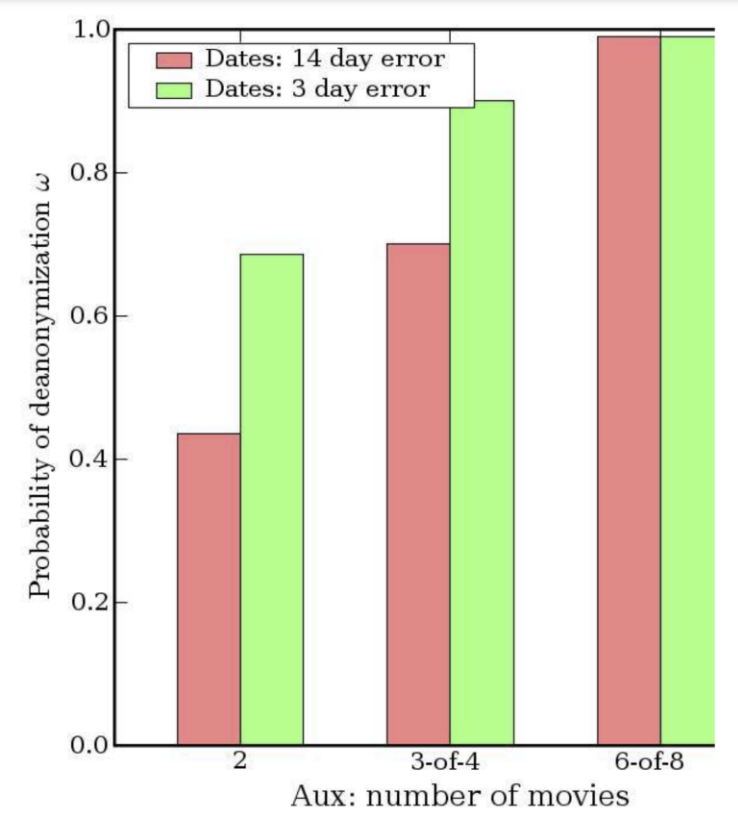
    log(7.75e9) = 32.9 bits
  - subject in the Netflix dataset?

    log(500000) = 18.9 bits



What is PII anyway?

- Both Netflix and the law refer to *personal identifiable information*
- Conventionally: name, government-issued identifiers, address, …
- Results of this attack: *"With 8 movie ratings (of which 2 may be completely wrong) and dates that may have a 14-day error, 99% of records be uniquely identified in the dataset. For 68%, two ratings and dates (with a 3-day error) are sufficient"*
- Netflix ended up settling a class-action lawsuit based on the Video Privacy Protection Act



Takeaways

- Policy may seem straightforward, but is difficult to enforce
- Heuristics are usually broken quickly
- Obscurity is never a good defense
- Need to be methodical and unambiguous about:
  - Defining security goals
  - Identifying a policy that is sufficient to achieve them
  - Developing a comprehensive method of enforcing the policy
  - **Proving** that the result matches the policy

Sneak peek: Differential Privacy

Goal: *Person's risk of privacy breach should not increase significantly due to their participation*

Policy: *Regardless of whether any single person is in the data, the output should remain about the same*

Enforcement: *Introduce carefully-designed randomness at key points in the computation*

Result: *Provable guarantee limiting what personal data can be learned via output*

This course

Look at security from the coder's perspective

We'll cover a range of security concerns

- Safety: *The code will never do something we deem "bad"*
- Isolation: *Untrusted code and data can't affect important state*
- Information Flow: *Confidential data remains that way*
- Privacy: *Don't jeopardize peoples' autonomy, control over their data*
- Authorization: *Only designated parties/code can obtain rights*
- Trust: *Leverage a small base to establish trust in a complete system, new parties*

Recurring themes

- Ways of specifying computations that are secure, i.e. *policies*
- Ways of ensuring that code meets policy, i.e. *enforcement*
- Establishing rigorous connections between policy, enforcement, and code

Logic and languages

Why is this an L&L elective?

Precise ways to write down policies

- Types, logical formulas, domain-specific languages
- Often devised for correctness, perfect for security also

Rigorous means of enforcement

- Static: verification, type checking
- Dynamic: runtime monitors, code instrumentation
- We will prove many of the approaches covered this semester

Learning objectives

After taking this course, you should:

- Be able to identify, formalize, and implement a range of practical security & privacy policies
- Understand the tradeoffs of different approaches to security & privacy, and how to use context-specific rationale to justify them
- Understand how general principles like least privilege, roots of trust, and complete mediation play a role in formulating and vetting defenses
- Be able to provide a formal security argument for several types of security mechanisms implemented in code

Logistics

- Website: https://cs.cmu.edu/~15316
- Contact: 15-316-course-staff@lists.andrew.cmu.edu
- Lecture: This room, same time, Tuesday/Thursday
  - Attendance expected, but not recorded
  - Piazza is not a substitute for attending lecture
- Anything not turned in in-class submit to Gradescope

- Office hours
  - My office, Mondays from 1:30-2:30
  - TAs in Gates Commons or CIC, details posted soon

Grading

- Breakdown:
  - 35% written homework
  - 35% labs
  - 15% final exam
  - 15% quizzes

Final letter grades

- Expect 90/80/70/60 thresholds
- Any variation will be applied consistently

- Written HW on average ~1.5 assignments every 2 weeks
- 2 labs
- ~8 quizzes
- Final is closed-notes
- Late assignments
  - 10% deduction per day
  - Lowest HW, lab grades dropped

Written homework (35%)

Focus on theory + fundamental skills

Handed out on Mondays, due Sunday evening

Grades based on:

- Correctness (obviously)
- How you present your reasoning

Strive for **clarity & conciseness**

- State your assumptions
- Show your steps
- Answers without justification will not receive full credit

Labs (35%)

Goal: Translate theory into something that works

- Design policies, formalize them, figure out how to implement enforcement mechanisms
- Learn to use new tools in the process

Grades are based on:

- Correct functionality
- Completeness, robustness of security mechanism
- Documentation, clarity of your solution

You are expected to complete labs indepdendently

- We're happy to provide guidance on solutions you devise
- We will not help you debug your code

Quizzes (15%)

Every 1.5 weeks:

- Quiz handed out at start of lecture, due by midnight
- Released on Canvas after lecture
- Ask questions during lecture!
- After lecture, you may only use lecture notes

Why?

- We expect you to attend lecture
- If you really can’t, let me know and we’ll figure something out
- Otherwise, skip at your own peril

Final Exam (15%)

Evidence of your ability to reason & apply main ideas from this course

- In-person, cumulative
- Questions resemble less time-intensive homework problems
- We provide a representative practice exam a week before the test

Not a check on your recall of minute details

- Exam comes with an extensive formula sheet
- You may bring 1 page of handwritten notes

Before Thursday

Make sure that you are enrolled in Gradescope, Canvas, Piazza sections

- Piazza signup: https://piazza.com/cmu/fall2022/15316
- Gradescope code: J37XN8
- Canvas link: https://canvas.cmu.edu/courses/31582

Answer Piazza poll about OH times

Read the syllabus, reach out if there are questions