15-316: Software Foundations of Security and Privacy

Introduction

Spring 2026

Course Staff

Justin Zou

Keya Mann

Sanjana Kuchibhotla

Yuchen Wang

Eleanor Li

Jackson Ma

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
- 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

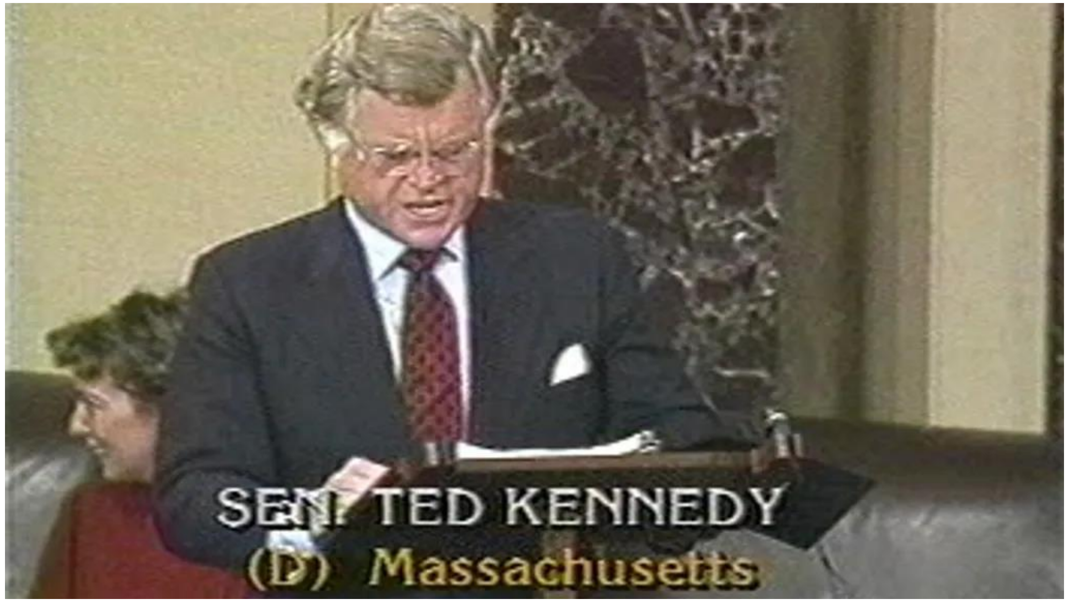
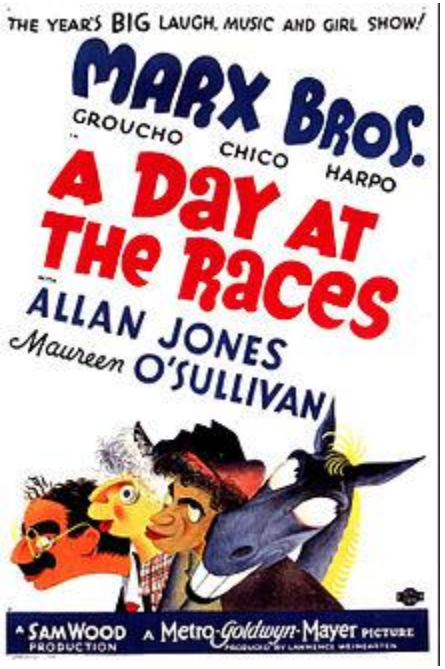


Image source: Associated Press, 1987

Damning revelations



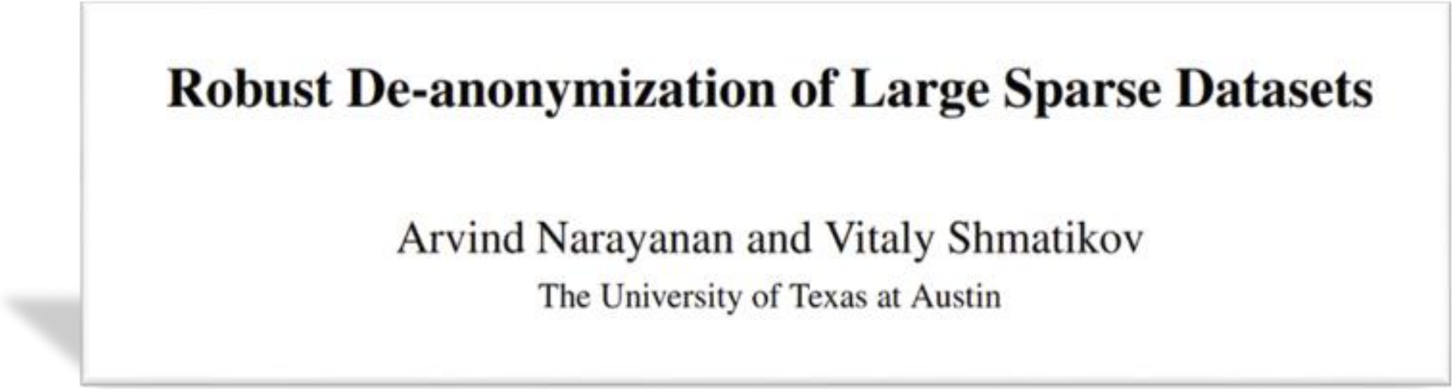
Video Privacy Protection Act of 1988

- 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	Jurassic Park	…	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

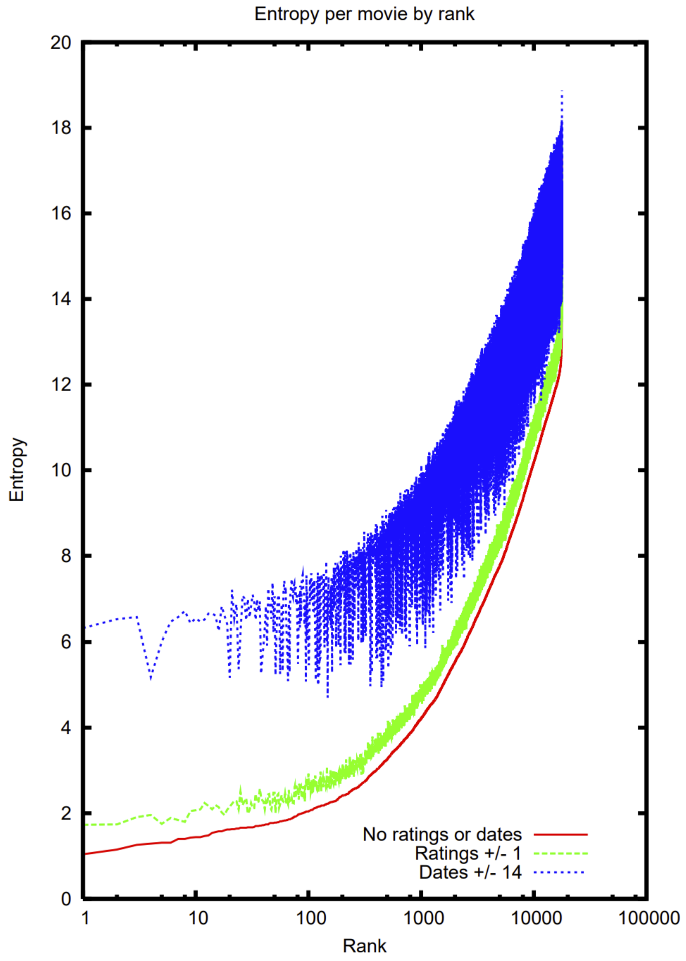
- *Entropy* is a measure of the uncertainty about a random outcome
- Defined as the expected negative logarithm of the probability, measured over all outcomes

$$H(X) = \mathbf{E}[-\log p(X)]$$

- Without any prior information about the outcome, how many bits do we need to uniquely identify a randomly-selected…
  - person on earth?

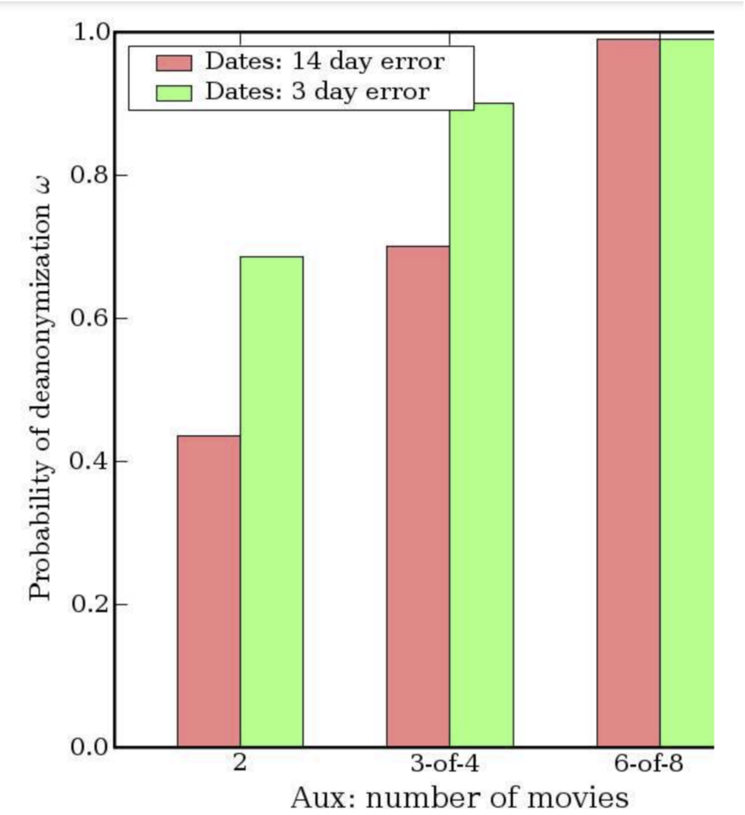
    log(7.75e9) = 32.9 bits
  - subject in the Netflix dataset?

    log(500000) = 18.9 bits



What is private information anyway?

- Both Netflix and the law refer to *personal identifying/identifiable information*
- Conventionally: name, unique 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 are 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

- Seemingly straightforward policy, surprisingly difficult to defend
- Need to be methodical about:
  - Defining security goals
  - Identifying a policy
  - Implementing enforcement
  - Demonstrating results

Sneak peek: Differential Privacy

Goal: *A person's risk of privacy breach should not increase because they participate*

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

Enforcement: *Introduce randomness at key points in computation*

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

This course

Security from a programmer’s standpoint

We’ll cover a range of 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: *Control over peoples’ data and how it’s used*
- Authorization: *Only designated actors/code can obtain rights*
- Trust: *Leverage a small base to establish trust in a complete system*

Recurring themes; ways of…

- specifying computations that are secure, i.e. *policy*
- ensuring that code meets policy, i.e. *enforcement*
- connecting the two rigorously, i.e. *semantics*

Logic and languages

Why is this a logic and languages elective?

Precise ways to write down policies

- Types, logical formulas, domain-specific languages
- Correctness and security go hand-in-hand

Enforcing them *rigorously*

- Static: verification, type checking
- Dynamic: runtime monitors, code instrumentation
- Either way, prove that the policy won't be violated

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 reason about which tradeoffs are justified
- Understand how general principles like least privilege, roots of trust, and complete mediation play a role in building defenses
- Be able to argue rigorously about software security mechanisms
- Understand the role of automated reasoning in analyzing security policies and mechanisms, and gain experience applying widely-used tools for this purpose

Logistics

- Website: https://cs.cmu.edu/~15316
- Contact: Piazza
- Lecture: HOA 160, 2:00-3:20 Tuesday/Thursday
  - Attendance expected, but not recorded
  - Piazza is not a substitute for attending lecture
- Submit everything to Gradescope

- Office hours
  - My office, Fridays from 1:00-2:30
  - TAs in Gates Commons or CIC, details posted soon

Grading

- Breakdown:
  - 40% written homework
  - 40% labs
  - 20% final exam

Final letter grades

- 90/80/70/60 thresholds
- Round up

- 5 written homeworks
- 3 labs
- Final exam during finals week
- Five late days, no more than 2 used on any one assignment

Written homework

Focus on theory + fundamental skills
1 week to complete
Due dates for the semester are on the course website

Grades based on:

- Correctness (obviously)
- Rigor
- Clarity

Rigor and clarity in this course:

- Formally state what you intend to show
- List any assumptions
- Show your steps, with appropriate justification

Labs

Translate theory into something that works

- Design a set of policies and a way of enforcing them
- Formalize both
- Implement them for the setting described in the lab
- Learn to use new tools in the process

Grades are based on:

- Correct functionality (evaluated by autograder)
- Completeness, robustness of security mechanism
- Documentation, clarity of your solution
- In-person comprehension check (~15 minute quiz)

Complete the labs independently!

- We can help with: understanding the setting/concepts, critiquing your approach
- We wont help with: debugging code, proposing an approach

Final Exam

Reason & apply main ideas from this course

- In-person, cumulative
- Questions resemble less time-intensive homework problems
- Representative practice exam released the last week of classes

Not a check on your recall of minute details

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

Use of AI tools

You **may** use AI to:

- Explain, answer questions about concepts covered in the course
- Check your understanding–but be careful, and check references!
- Generate practice exercises
- Help typeset work that you've already completed

You **may not** use AI to:

- Write *any* code for the labs
- Write test cases that you hand in for a grade
- Provide answers for written homework
- Generally: complete graded work for you

Before Thursday

Make sure that you are enrolled in Gradescope and Piazza sections

- Piazza signup: https://piazza.com/cmu/spring2026/15316
- Gradescope code: 2D2XJ5